



OPEN

An improved reversible watermarking scheme using embedding optimization and quaternion moments

Mohamed Amine Tahiri¹, Hicham Karmouni², Mhamed Sayyouri¹, Hassan Qjidaa³, Musheer Ahmad⁴, Mohamed Hammad⁵, Paweł Pławiak^{6,7}, Osama Alfarraj⁸ & Ahmed A. Abd El-Latif^{9,10}✉

Digital watermarking of images is an essential method for copyright protection and image security. This paper presents an innovative, robust watermarking system for color images based on moment and wavelet transformations, algebraic decompositions, and chaotic systems. First, we extended classical Charlier moments to quaternary Charlier moments (QCM) using quaternion algebra. This approach eliminates the need to decompose color images before applying the discrete wavelet transform (DWT), reducing the computational load. Next, we decompose the resulting DWT matrix using QR and singular value decomposition (SVD). To enhance the system's security and robustness, we introduce a modified version of Henon's 2D chaotic map. Finally, we integrate the arithmetic optimization algorithm to ensure dynamic and adaptive watermark insertion. Our experimental results demonstrate that our approach outperforms current color image watermarking methods in security, storage capacity, and resistance to various attacks, while maintaining a high level of invisibility.

Keywords Henon chaotic map, Quaternion moments, Digital image watermarking, Optimization algorithm

Currently, the security of multimedia data in all forms (images, videos, and audio) plays an important role in all domains, especially for military or medical domains that require a very high level of confidentiality. To prevent illicit acts such as hacking, falsification, or unauthorized use of sensitive information, major security concerns must be addressed¹.

Images, as carriers of crucial information, are increasingly widespread and stored across networks. This expansion has drawn the attention of researchers to issues relating to their transmission and preservation. The fundamental solution is to encrypt or digitally watermark these images before transferring them^{2–4}. This approach aims to ensure the confidentiality and security of images, prevent unauthorized alteration, and enable authentication of their source. It thus meets the need for data protection and image integrity verification in an ever-growing digital environment⁵. In this context, cryptography was the first proposal to secure the transfer of digital color images. Today, modern encryption algorithms, with very sensitive and long security keys, can ensure the confidentiality and security of images. However, once the image is decrypted, it is no longer protected and can be distributed or modified in an illegal way. Information hiding, and more specifically the insertion of hidden data in the images, can be an answer to this problem^{6–8}. Indeed, the insertion of a watermark in an

¹Engineering, Systems and Applications Laboratory, National School of Applied Sciences, Sidi Mohamed Ben Abdellah University, Fez, Morocco. ²National School of Applied Sciences, Cadi Ayyad University, 40000 Marrakech, Morocco. ³Laboratory of Electronic Signals and Systems of Information, Sidi Mohamed Ben Abdellah-Fez University, Fez, Morocco. ⁴Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India. ⁵Department of Information Technology, Faculty of Computers and Information, Menoufia University, Shibin El Kom 32511, Egypt. ⁶Department of Computer Science, Faculty of Computer Science and Telecommunications, Cracow University of Technology, Warszawska 24, 31-155 Krakow, Poland. ⁷Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland. ⁸Computer Science Department, Community College, King Saud University, 11437 Riyadh, Saudi Arabia. ⁹Jadara University Research Center, Jadara University, Irbid, Jordan. ¹⁰Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shibin el Kom 32511, Egypt. ✉email: a.rahiem@gmail.com

image allows us to authenticate it and to guarantee its integrity. In recent years, significant advances have been made in the field of digital watermarking applied to color images. Table 1 provides an overview of the research and work carried out in this specific field. This work shows a growing interest in the use of digital watermarking methods, particularly for color images, to guarantee the security, confidentiality, and authenticity of visual data. This development reflects the growing importance of copyright protection and image security in various fields of application, such as medicine and military security.

We can see that copyright protection with color images has become an increasingly pressing challenge in this day and age, given that many organizations' trademarks, logos, and information to be hidden are in color. In this context, it is worth mentioning that color watermarking has two advantages over grayscale watermarking: (i) It allows a greater amount of data to be hidden. (ii) It achieves a higher level of realism since color perception depends not only on brightness but also on chrominance^{9,10}.

After conducting an exhaustive review of the relevant literature and highlighting digital watermarking methods, we concluded that one of the most significant obstacles facing researchers in the field of digital watermarking is the development of an algorithm that manages to effectively balance the various properties, including imperceptibility, capacity, robustness, and data security. In this publication, we present a hybrid approach that combines the principles of digital watermarking and encryption. Our watermarking method is essentially based on the use of QCM, DWT, SVD, QR, and modified Henon cards. This innovative approach combines these elements to ensure the security and robustness of the watermark while preserving its invisibility in color images. We will go into more detail on the various stages of this method and provide an assessment of its performance through in-depth simulations.

To explain our new watermarking system in depth, we start by extending classical Charlier Moments (CM) to the QCM using quaternion algebra. This extension allows us to holistically represent color images without having to decompose their three components (red, green and blue) and without losing any information. Next, the resulting matrix of QCMs is subjected to decomposition in the DWT. This approach allows us to avoid decomposing the host and watermark images into three distinct RGB planes, reducing both decomposition time and computational complexity. We then decompose the DWT-generated matrix using both QR and SVD transformations. It is important to note that these QR and SVD decompositions are particularly effective in detecting important image features, thus reducing the amount of information to be analyzed in the image. To enhance the security and reliability of our system, we introduce a modified version of Henon's 2D chaotic map, which we refer to in this paper as 2D-FrMHM. This modified version offers more parameters than the classical map, thus enhancing the overall safety of the system. Finally, to guarantee a dynamic and adaptive scaling factor when inserting the watermark, we use the Arithmetic Optimization Algorithm (AOA). This final step contributes to improving the overall robustness of our watermarking system.

Essential contributions

The main contributions of this research.

- 1. Introduction of Quaternion Moments (QCM): This study introduces QCM as a novel representation for color images. QCM not only preserves image integrity but also reduces computational complexity significantly, marking a significant advancement in image representation.
- 2. Modification of Chaotic System: The research presents a novel modification to a chaotic system, enhancing the system's security and expanding its parameterization possibilities. This modification represents a noteworthy advancement in chaotic system design.
- 3. Integration of Arithmetic Optimization Algorithm (AOA): The incorporation of AOA facilitates dynamic and adaptive scaling factor selection, enhancing the flexibility and efficiency of the watermarking system.
- 4. Development of Hybrid Watermarking Method with Color Image Encryption: A key contribution is the proposal of a hybrid method that combines watermarking and color image encryption. This approach addresses the dual requirements of copyright protection and medical information confidentiality, representing a significant advancement in image security techniques.

Objectives	Approaches	Treatment domain
Suggests a novel approach for color image blind watermarking ¹¹	Discrete Fourier transform (DFT), Arnold transformation (AT)	Spatial and transform
Propose a semi blind color image watermarking system ¹²	Quaternion Hadamard transform, Schur decomposition, Zernike moments	Transform
Propose a robust non-blind watermarking method ¹³	DCT-DWT and AT	Transform
Propose a reliable and flexible watermarking system ¹⁴	RDWT, SVD, AT and artificial bee colony algorithm	Transform
Propose a double-blind watermarking ¹⁵	DWT and least significant bits	Spatial and transform
Propose a blind watermarking method based on chaotic encryption ¹	DCT, DWT, AT and chaotic encryption	Transform
Propose a reversible watermarking algorithm that ensures copyright protection of color medical images ¹⁶	Zernike moment and Haar wavelet transform	Transform
Propose a quaternary watermark of a color image by integrating color watermarks ¹⁷	Schur decomposition and Affine transform	Transform
Propose an approach to blindly watermarking digital color images using image correction and eigenvalue decomposition ¹⁸	EVD, HT and Affine transform	Transform

Table 1. Watermark articles of color images with their objectives, approaches used, and processing domain.

General structure

We structured the rest of this work as follows: in “Preliminaries”, we present the theoretical background of the research. We devote “Fast computation of discrete orthogonal quaternary Charlier moments” to the presentation of quaternion orthogonal discrete Charlier moments. In “Improved reversible watermarking scheme”, we will present the proposed scheme for watermarking color images. In “Simulations and findings”, we illustrate the simulation results. The last section concludes the work.

Preliminaries

In this section, we outline the QR, SVD and a modified version of the 2D-Henon map, referred to in the remainder of this article as (2D-FrMHM), which will be implemented in the new watermarking system to improve its overall performance.

QR decomposition

QR is a matrix factorization where a real matrix is represented as the result of multiplying an orthogonal matrix Q by an upper triangular matrix R (Eq. 1)^{19,20}.

$$A = QR \quad (1)$$

Note that the R -matrix contains more significant elements that represent most of the energy of the signal (image) after the transformation. Experimentation and analysis revealed that the larger element provides numerical stability to external disturbances. In information security and data hiding technologies, A-matrix decomposition has the potential to increase anti-attack performance^{19,20}.

Singular value decomposition

SVD is an algebraic approach in which matrices are treated based on their eigenvectors. The singular vector of the matrix can be obtained by SVD, keeping the correlation of the rows or columns of the original matrix²¹. The SVD decomposition of a matrix A of size $N \times N$ is given by Eq. (2) with U and V , two orthogonal matrices, and S a diagonal matrix.

$$USV^T = SVD(A) \quad (2)$$

$$S = \text{diag}(\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_n) \quad (3)$$

The diagonal elements of $S = \{\sigma_1, \sigma_2, \sigma_3, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_n\}$ are singular values of matrix A .

Modified chaotic system

Chaotic systems²² are one of the most common methods used to contribute to the field of information security^{23–25}. Mathematically, the 2D fractional Henon map is defined by Eq. (4), with $(x, y) \in \mathbb{R}^2$, $(\alpha, \gamma) \in \mathbb{R}^2$ and the fractional order $\nu \in [0, 1]$ ²⁶.

$$\begin{cases} x(n) = x(0) + \frac{1}{\Gamma(\nu)} \sum_{i=1}^n \frac{\Gamma(n-i+\nu)}{\Gamma(n-i+1)} (y(i-1) + 1 - \alpha x^2(i-1) - x(i-1)) \\ y(n) = y(0) + \frac{1}{\Gamma(\nu)} \sum_{i=1}^n \frac{\Gamma(n-i+\nu)}{\Gamma(n-i+1)} (\beta x(i-1) - y(i-1)) \end{cases} \quad (4)$$

The chaotic characteristic of the map represented in Eq. (4) undergoes a modification due to the amplification of numerical errors when calculating output values for high orders. This amplification arises from the presence of the non-elementary analytical function gamma, as shown in Table 2. This modification is highlighted using the following parameters $[\alpha, \beta, x(0), y(0), \nu] = [1.95, 0.001, 0.009, 0, 0.98]$.

Next, we introduce a 2D-FrMHM that addresses instability issues during computation by substituting $\frac{\Gamma(n-i+\nu)}{\Gamma(n-i+1)}$ with $e^{\ln(x)}$. Moreover, to improve the security level, we will increase the complexity of the map by adding two additional parameters φ_1, φ_2 that will extend the space of the security keys. Indeed, the 2D-FrMHM is defined by Eq. (5)²⁷.

where $(x, y) \in \mathbb{R}^2$, $(\alpha, \gamma) \in \mathbb{R}^2$ and $\nu \in [0, 1]$ are the fractional orders, and $|\cos(i)|$ is the absolute value of $\cos(i)$.

The order (n)	n = 171	n = 172	n = 173	n = 2000
x	0.5863	Inf	Inf	Inf
y	0.3746	Inf	Inf	Inf

Table 2. Values of the 2D-FrMHM calculated for $n = 0 : 2000$.

$$\begin{cases} x(n) = x(0) + \frac{1}{\Gamma(v)} \sum_{i=1}^n A_1 \times (1 - \varphi_1 \times |\cos(i)|) \times \exp(\ln(\Gamma(n-i+v)) - \ln(\Gamma(n-i+1))) \\ y(n) = y(0) + \frac{1}{\Gamma(v)} \sum_{i=1}^n A_2 \times (1 - \varphi_2 \times |\cos(i)|) \times \exp(\ln(\Gamma(n-i+v)) - \ln(\Gamma(n-i+1))) \end{cases} \quad (5)$$

$$\begin{cases} A_1 = y(i-1) + 1 - \alpha x^2(i-1) - x(i-1) \\ A_2 = \alpha x(i-1) - y(i-1) \end{cases} \quad (6)$$

To assess and visually represent the performance and effectiveness of the modified Henon map, we generate plots of the $x(n)$ and $y(n)$ coordinates of the map and the corresponding phase space as functions of the iteration number " n ", using the same parameter values employed in the traditional 2D Henon map ($[\alpha, \beta, x(0), y(0), \varphi_1, \varphi_2, v] = [1.95, 0.001, 0.009, 0, 0.98]$).

Figure 1c illustrates the 2D-FrMHM by individual points in space, creating a shape closely resembling a half-oval, while Fig. 1a,b plot the two $x(n)$ and $y(n)$ coordinates as a function of the number of iterations " n ", showing that they remain stable whatever " n ". While Fig. 1d–f represent the classic Henon instability for large sizes. These observations reinforce the idea that the modified system exhibits both chaotic behavior and remarkable stability, particularly for high values of " n ". This suggests that our stabilization approach is effective in resolving the numerical instability problems typically encountered in calculations involving high values of " n ". Importantly, this stability is crucial to ensure the reliability of our method for digitally watermarking color images, particularly when applied to large images or applications requiring high accuracy. As a result, our approach offers a robust solution for inserting digital watermarks into color images while maintaining a chaotic behavior desirable for system safety and robustness^{28,29}.

Fast computation of Charlier polynomial (CP)

The CP is defined by Eq. (7), where " x " and " n " represent the variable and the CP order, while " a " is the control parameter.

$$CP_n^a(x) = {}_2F_0\left(-n, -x; -\frac{1}{a}\right); \quad x, n \in [0, \infty] \quad (7)$$

Iterative computation of CP^{30} , whether with respect to order n or the variable x , generates the numerical instability of these polynomials, as highlighted in Figs. 2 and 3. This instability results from the propagation of numerical errors and can present challenges when applying these methods to large images in the security domain. To overcome this limitation, researchers have adopted the Gram–Schmidt Ortho-normalization Process (GSOP)^{31–33}. However, this method is still limited by the computational time, which is characterized by exponential behavior with an increment of n . As an example, the elapsed time in seconds (s) using GSOP for the case where $N = 100$ is 0.2546 s and for $N = 1000$ is 4.7835e + 02 s. Using the recursive method or the GSOP method to figure out CP causes problems with stability and the time to figure out CP.

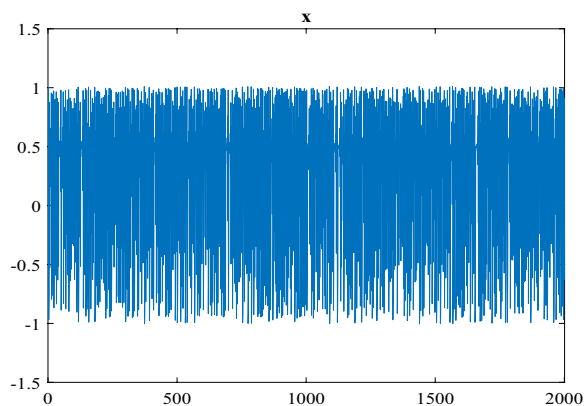
The fundamental idea for solving the problems of numerical instability associated with CP calculation lies in the adoption of an innovative and efficient algorithm³⁴. This algorithm is designed to guarantee the stable calculation of CP values, which is essential for our method of digitally watermarking color images. Its efficiency is based on two key principles: the notion of symmetry and the simultaneous use of standard recurrence relations associated with n and x . By adopting this method, our digital watermarking system for color images can effectively exploit the advantages of CP while avoiding the problems of numerical instability. This enhances the reliability and robustness of our approach, making it suitable for a wide range of applications, including the digital watermarking of large color images in fields requiring high precision and enhanced security^{35,36}. It is important to note that this approach has already been successfully employed to stabilize other polynomials in previous works in the literature³⁵.

Practically, after specifying the surface of CP calculations by determining the exact value of n , the plane of CP is divided into two parts having the shape of a triangle bounded by the diagonal $n = x$, as shown in Fig. 4. Thus, the calculation of the values of CP is performed in five steps, as shown in the pseudocode below (Algorithm 1), where $\omega_{CP}(x)$ and $\rho_{CP}(n)$ are the weight function and the quadratic norm respectively:

$$\omega_{CP}(x) = \frac{e^{-a} a^x}{\Gamma(x+1)} \quad (8)$$

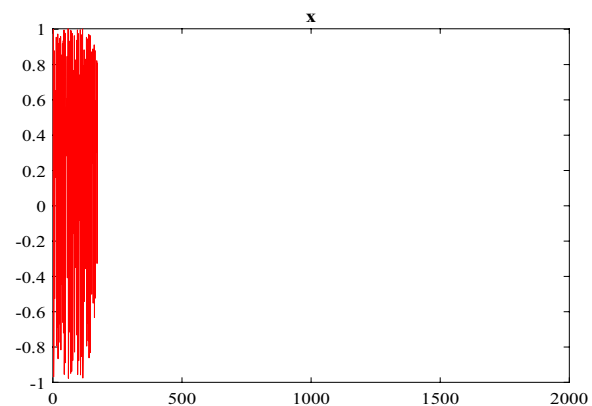
$$\rho_{CP}(n) = \frac{\Gamma(n+1)}{a^n} \quad (9)$$

The modified 2D Henon (2D-FrMHM)

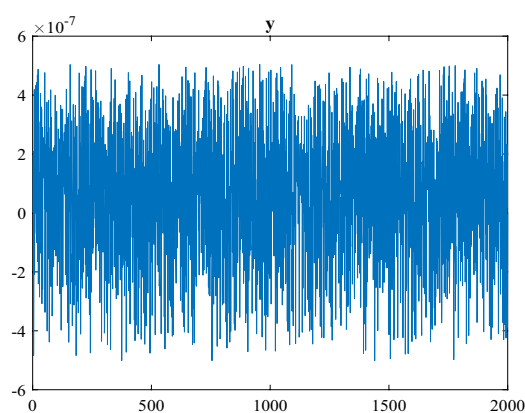


(a)

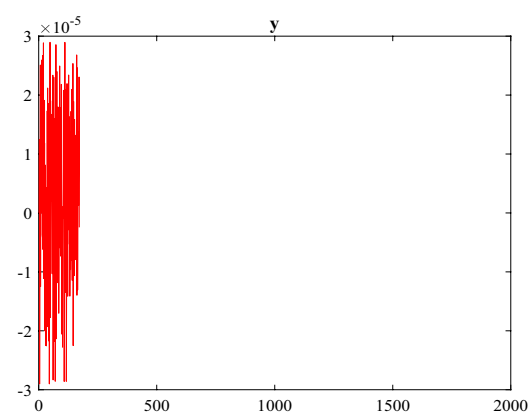
2D Henon classic



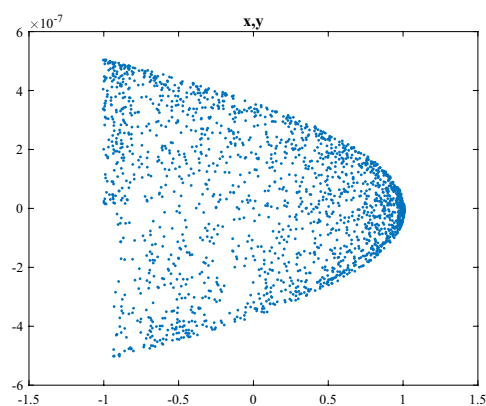
(d)



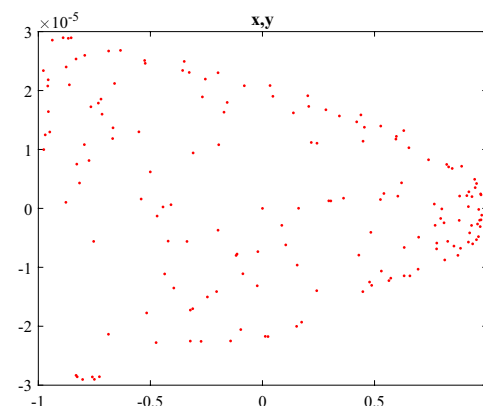
(b)



(e)



(c)



(f)

Figure 1. (a,d) First coordinate $x(n)$. (b,e) Second coordinate $y(n)$. (c,f) The phase space (x, y) .

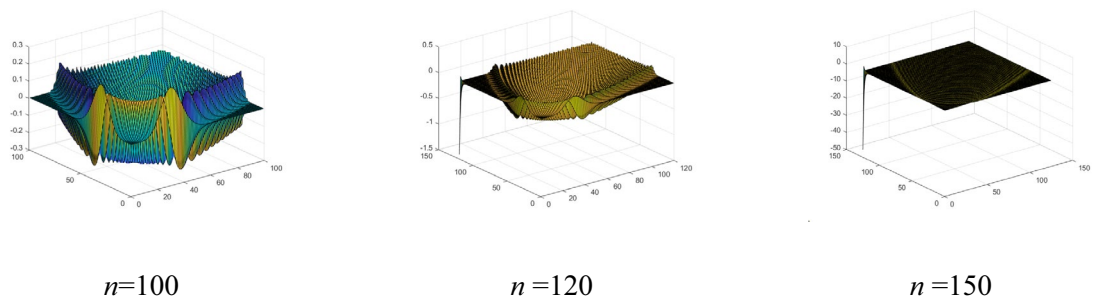


Figure 2. For the case $a=40$, 3D traces of CP versus n with different orders.

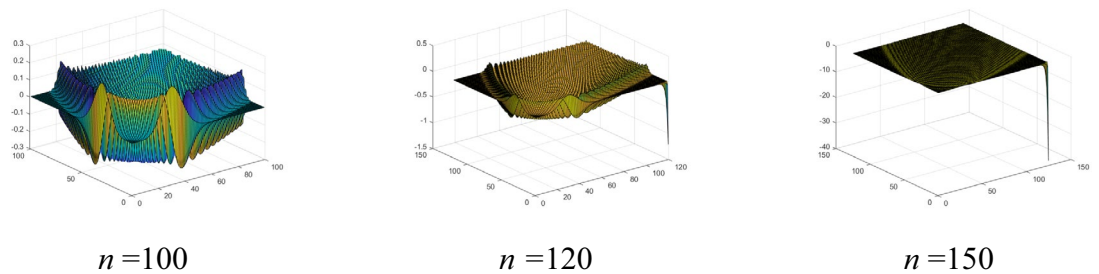


Figure 3. For the case $a=40$, 3D traces of CP versus x with different orders.

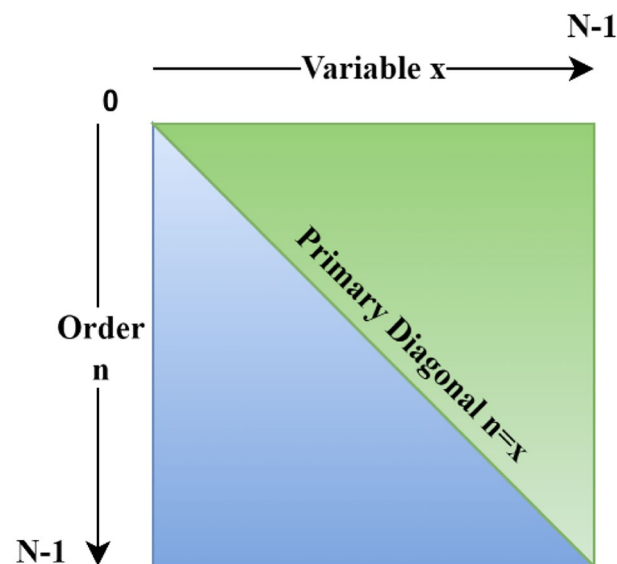


Figure 4. Regions of symmetry regarding to the diagonal $n=x$.

Inputs: CP control parameter, $N_{\max}$.

Outputs: CP matrix.

Step 1: The values of $\tilde{C}P_0^a(0)$ are computed using the following equation:

$$\tilde{C}P_0^a(0) = e^{-a/2} \quad (10)$$

Step 2: The values of $\tilde{C}P_0^a(x)$ within the range $x = 1, 2, 3, 4, 5, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_0^a(x) = \sqrt{\frac{\omega_{CP}(x)}{\rho_{CP}(0)}} \quad (11)$$

Step 3: The values of $\tilde{C}P_1^a(x)$ within the range $x = 1, 2, 3, 4, 5, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_1^a(x) = \frac{a-x}{a} \sqrt{\frac{\omega_{CP}(x)}{\rho_{CP}(1)}} \quad (12)$$

Step 4: The values of $\tilde{C}P_n^a(n)$ within the range $n = 2, 3, 4, 5, \dots, N_{\max}$ and $x = n, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_n^a(x) = \frac{a-x+n-1}{a} \sqrt{\frac{a}{n}} \tilde{C}P_{n-1}^a(x) - \sqrt{\frac{n-1}{n}} \tilde{C}P_{n-2}^a(x) \quad (13)$$

Step 5: The values of $\tilde{C}P_n^a(n)$ within the range $n = 0, 1, 2, \dots, N_{\max}$ and $x = n, \dots, N_{\max}$ are computed using the following equation:

$$\tilde{C}P_n^a(x) = \tilde{C}P_x^a(n) \quad (14)$$

Algorithm 1: Fast computation of CP values³⁴.

Step 1: The values of $\tilde{C}P_0^a(0)$ are computed using the following equation:

$$\tilde{C}P_0^a(0) = e^{-a/2} \quad (10)$$

Step 2: The values of $\tilde{C}P_0^a(x)$ within the range $x = 1, 2, 3, 4, 5, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_0^a(x) = \sqrt{\frac{\omega_{CP}(x)}{\rho_{CP}(0)}} \quad (11)$$

Step 3: The values of $\tilde{C}P_1^a(x)$ within the range $x = 1, 2, 3, 4, 5, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_1^a(x) = \frac{a-x}{a} \sqrt{\frac{\omega_{CP}(x)}{\rho_{CP}(1)}} \quad (12)$$

Step 4: The values of $\tilde{C}P_n^a(n)$ within the range $n = 2, 3, 4, 5, \dots, N_{\max}$ and $x = n, \dots, N-1$ are computed using the following equation:

$$\tilde{C}P_n^a(x) = \frac{a-x+n-1}{a} \sqrt{\frac{a}{n}} \tilde{C}P_{n-1}^a(x) - \sqrt{\frac{n-1}{n}} \tilde{C}P_{n-2}^a(x) \quad (13)$$

Step 5: The values of $\tilde{C}P_n^a(n)$ within the range $n = 0, 1, 2, \dots, N_{\max}$ and $x = n, \dots, N_{\max}$ are computed using the following equation:

$$\tilde{C}P_n^a(x) = \tilde{C}P_x^a(n) \quad (14)$$

Fast computation of discrete orthogonal quaternary Charlier moments

The quaternion model is an example of a mathematical approach that could be used effectively for digital color image processing³⁷, as it generalizes grayscale modelling (on R or C) and treats color images holistically as an individual quaternion without decomposition into three RGB planes^{38,39}. The quaternion representation of a digital color image $f(x, y)$ is defined as follows:

$$f(x, y) = f_{RED}(x, y)i + f_{GREEN}(x, y)j + f_{BLUE}(x, y)k \quad (15)$$

The QCM are calculated from Eq. (15), knowing that the CP are calculated by algorithm 1.

$$QCM_{nm}(f) = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (f_{Red}(x, y)i + f_{Green}(x, y)j + f_{Blue}(x, y)k) \times (\tilde{C}P^a(x)\tilde{C}P^a(y)) \times \mu \quad (16)$$

with $\mu = \frac{-(i+j+k)}{\sqrt{3}}$. Taking into consideration the definition of μ , Eq. (16) is simplified as follows:

$$\begin{aligned} QCM_{nm}(f) = & \frac{1}{\sqrt{3}} \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (f_{Red}(x, y) + f_{Green}(x, y) + f_{Blue}(x, y)) \times (\tilde{C}P^a(x)\tilde{C}P^a(y)) \right] \\ & - \frac{1}{\sqrt{3}} i \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (f_{Green}(x, y) - f_{Blue}(x, y)) \times (\tilde{C}P^a(x)\tilde{C}P^a(y)) \right] \\ & - \frac{1}{\sqrt{3}} j \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (f_{Blue}(x, y) - f_{Red}(x, y)) \times (\tilde{C}P^a(x)\tilde{C}P^a(y)) \right] \\ & - \frac{1}{\sqrt{3}} k \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (f_{Red}(x, y) - f_{Green}(x, y)) \times (\tilde{C}P^a(x)\tilde{C}P^a(y)) \right] \end{aligned} \quad (17)$$

The 2D moments (M_{nm}) of $f(x, y)$ of size $N \times N$ using CP are obtained by the following equation^{35,40,41}:

$$M_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \tilde{C}P_n^{a1}(x) \times \tilde{C}P_m^{a2}(y) \times f(x, y) \quad (18)$$

Using Eq. (18) to calculate moments generates a considerable computational load, making the process intensive in terms of computing resources. Therefore, to overcome this computational complexity, we opted for an alternative matrix approach.

$$M = CP_n^{a1T} \times F \times CP_m^{a2} \quad (19)$$

where M , CP_n^{a1} , CP_m^{a2} and F is the matrix form of M_{nm} , $\tilde{C}P_n^{a1}(x)$, $\tilde{C}P_m^{a2}(y)$, and $f(x, y)$.

Using Eq. (19), we obtain the simplified matrix version of QCM:

$$QCM_{nm}(f) = \frac{1}{\sqrt{3}} [M_R + M_R + M_R] - \frac{1}{\sqrt{3}} i [M_G + M_B] - \frac{1}{\sqrt{3}} j [M_B + M_R] - \frac{1}{\sqrt{3}} k [M_R + M_G] \quad (20)$$

In this equation, M_R , M_G and M_B represent Charlier's conventional discrete orthogonal moments for the red, green and blue channels, respectively. Equation (20) can be reformulated as the following formula:

$$QCM_{nm}(f) = D_0 + iD_1 + jD_2 + kD_3 \quad (21)$$

$$\begin{cases} D_0 = \frac{1}{\sqrt{3}} [M_R + M_R + M_R]; & D_1 = -\frac{1}{\sqrt{3}} [M_G + M_B] \\ D_2 = -\frac{1}{\sqrt{3}} j [M_B + M_R]; & D_3 = -\frac{1}{\sqrt{3}} k [M_R + M_G] \end{cases} \quad (22)$$

After the calculation of the $QCM_{nm}(f)$ moments, we present the inverse form of $IQCM_{nm}(f)$ (reconstruction of the 2D signal).

$$\hat{F} = CP_n^{a1} \times M \times CP_m^{a2T} \quad (23)$$

Utilizing Eqs. (17) and (23), we can now demonstrate the reverse computation of $QCM_{nm}(f)$.

$$\begin{aligned}
IQC_{nm}(f) = & \frac{1}{\sqrt{3}} \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (D_1 + D_2 + D_3) \times (\tilde{C}P^a(x) \tilde{C}P^a(y)) \right] \\
& - \frac{1}{\sqrt{3}} i \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (D_0 + D_2 - D_3) \times (\tilde{C}P^a(x) \tilde{C}P^a(y)) \right] \\
& - \frac{1}{\sqrt{3}} j \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (D_0 - D_1 + D_3) \times (\tilde{C}P^a(x) \tilde{C}P^a(y)) \right] \\
& - \frac{1}{\sqrt{3}} k \left[\sum_{x=0}^{N-1} \sum_{y=0}^{M-1} (D_0 + D_1 - D_2) \times (\tilde{C}P^a(x) \tilde{C}P^a(y)) \right]
\end{aligned} \quad (24)$$

$$\begin{aligned}
IQC_{nm}(f) = & \frac{1}{\sqrt{3}} [\hat{D}_1 + \hat{D}_2 + \hat{D}_3] - \frac{1}{\sqrt{3}} i [\hat{D}_1 + \hat{D}_2 + \hat{D}_3] - \frac{1}{\sqrt{3}} j [\hat{D}_0 - \hat{D}_1 + \hat{D}_3] \\
& - \frac{1}{\sqrt{3}} k [\hat{D}_0 + \hat{D}_1 - \hat{D}_2]
\end{aligned} \quad (25)$$

To illustrate the benefits and interest of extending classical Charlier moments to QCM moments, we conducted a visual evaluation using an arbitrary method of color image reconstruction from an MRI image of size 1024 (this image is selected from the database⁴²). Figure 5 shows the reconstruction of the MRI image using a Charlier control parameter $a = 512$ for various orders ranging from $n = 80$ to $n = 1024$. The results of this evaluation demonstrate that QCMs outperform classical Charlier moments. Furthermore, these results indicate that the QCMs do not exhibit any loss of information.

Having outlined the theoretical part of the paper, we will now present the digital watermarking scheme we have developed.

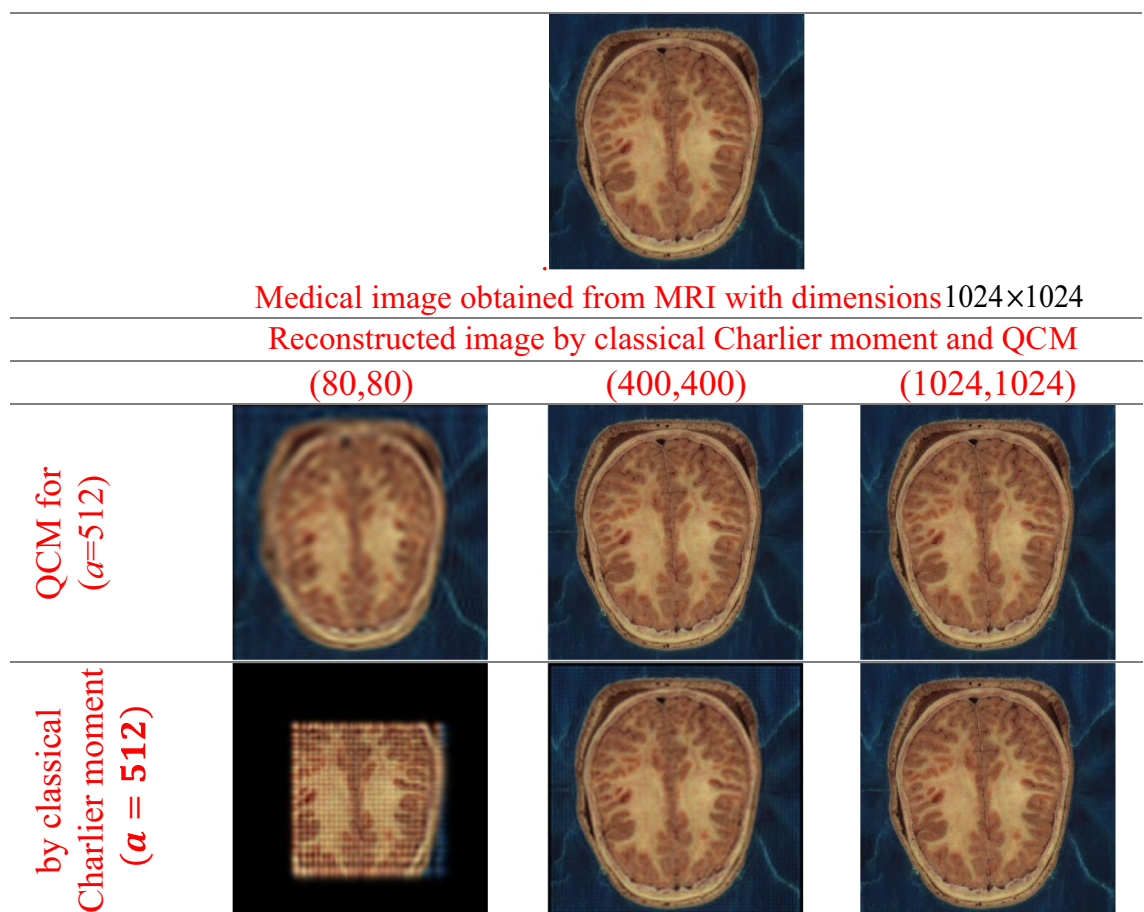


Figure 5. Comparative evaluation of medical image reconstruction using classic Charlier moments and QCM.

Improved reversible watermarking scheme

In this section, the QCM, DWT, QR, SVD and 2D-FrMHM are used to present a new improved reversible watermarking scheme. Figure 6 provides an overview of the proposed system (the images used in this figure are selected from database Ref.⁴²).

Proposed watermark scheme for color images

This phase consists of several successive steps, which generate watermarked color images from the original images and watermarks. A detailed description is presented in Fig. 7 (the images used in this figure are selected from database Ref.⁴² and website Ref.⁴³).

Watermark insertion process

Step 1: Calculate the moments of the input images using Eq. (24). This step eliminates the need to decompose the input images before applying DWT. This approach significantly reduces the computation time. In addition, the CP parameters a_1 and a_2 are used to increase the extent of the available security key space (KEY1).

Step 2: Decompose the image $I_H(x, y)$ into LL_{Hk} , LH_{Hk} , HL_{Hk} and HH_{Hk} by K-DWT, where $k = \log_2 \frac{M}{N}$.

Step 3: Decompose the resulting image LL_{Hk} into two matrices Q_H and R_H , as shown in Eq. (29), while considering the size of LL_{Hk} ; $\left(\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}\right)$.

$$Q_H \times R_H = QR(LL_{Hk}). \quad (26)$$

Step 4: Decompose the matrix R_H into three matrices U_H , S_H and V_H based on SVD decomposition as shown in Eq. (30), while considering the size of S_H ; $\left(\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}\right)$.

$$U_H \times S_H \times V_H^T = SVD(R_H) \quad (27)$$

Step 5: Encrypt the S_H matrix using 2D-FrMHM. To enhance the security of the proposed digital watermarking system, we implemented two crucial steps:

- (a) Confusion process: In this step, we interchange the positions of the values within S_H to generate matrix S_{H_2} , which serves as the representation of the permuted S_{H_1} . To accomplish this, we use two chaotic sequences $X(i)$ and $Y(j)$ defined in Eq. (5) to generate the following two vectors.

$$\begin{cases} X(i) = [x(1); x(2); x(3); \dots; x(M \times M)] \\ Y(j) = [y(1); y(2); y(3); \dots; y(M \times M)] \end{cases} \quad (28)$$

The two resulting vectors are arranged in ascending order and saved in variables denoted as $X^*(i)$ and $Y^*(j)$:

$$\begin{cases} X^*(i) = [x^*(1); x^*(2); x^*(3); \dots; x^*(M \times M)] \\ Y^*(j) = [y^*(1); y^*(2); y^*(3); \dots; y^*(M \times M)] \end{cases} \quad (29)$$

It is important to note that to guarantee the reversibility of the process, $L_x(i)$ and $L_y(j)$ must receive the index from which $X^*(i)$ and $Y^*(j)$ originated, for the change to be reversible. After completing the preparation of the chaotic sequences. We convert the matrix S_H into a 1D vector, then rearrange the elements of this vector according to $L_x(i)$ to obtain the $S_{H_1} = \{S_{H_1}(1), S_{H_1}(2), S_{H_1}(3), \dots, S_{H_1}\left(\frac{M}{2^{k+1}} \times \frac{M}{2^{k+1}}\right)\}$ sequence. This sequence is transformed into a 2D matrix $S_{H_1} = \{S_{H_1}(x, y)\}_{x,y=1}^{\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}}$. This step is performed for the S_{H_1} matrix, using $L_y(j)$ to make $S_{H_2} = \{S_{H_2}(x, y)\}_{x,y=1}^{\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}}$ (S_{H_1} scrambled).

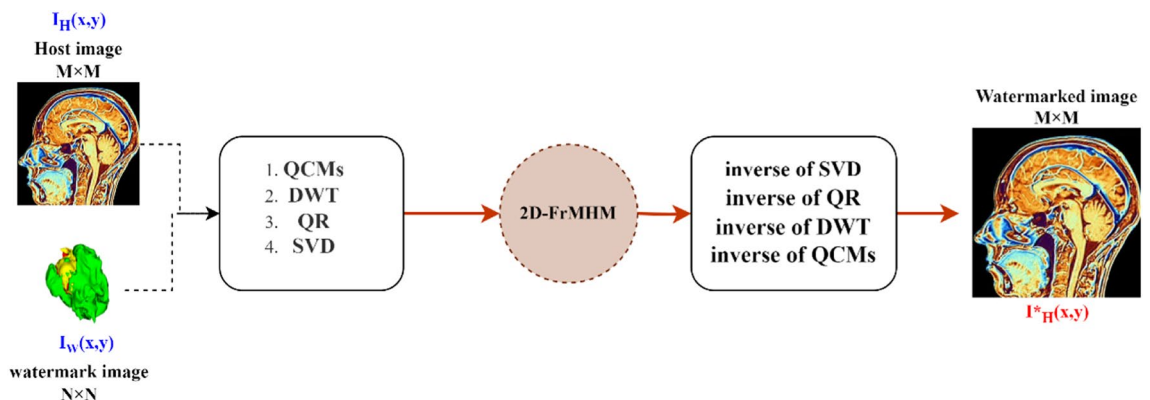


Figure 6. General overview of improved reversible watermarking scheme.



Figure 7. Watermark incorporation procedure.

- (b) Diffusion process: During this crucial stage of the process, the values of the S_{H_2} matrix undergo modifications to give rise to the encrypted matrix ES_H . This process is orchestrated by the use of two chaotic sequences presented in Eq. (5) ($X(i)$ and $Y(j)$), where they are rounded off to the nearest integer ($X_1(i) = \text{floor}X(i)$ and $Y_1(j) = \text{floor}Y(j)$).

The XOR function ($\oplus$) is used to combine the two sequences $X_1(i) = [x_1(1), x_1(2), x_1(3), \dots, x_1(\frac{M}{2^{k+1}} \times \frac{M}{2^{k+1}})]$ and $Y_1(i) = [Y_1(1), Y_1(2), Y_1(3), \dots, Y_1(\frac{M}{2^{k+1}} \times \frac{M}{2^{k+1}})]$, and the result is then resized to form a 2D matrix $T = \{T(x, y)\}_{x, y=1}^{\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}}$.

$$ES_H = \{S_{H_2}(x, y)\}_{x, y=1}^{\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}} \oplus \{T(x, y)\}_{x, y=1}^{\frac{M}{2^{k+1}}, \frac{M}{2^{k+1}}} \quad (30)$$

Before proceeding to the step of inserting $I_W(x, y)$ into $I_W(x, y)$, it should be noted that the image $I_W(x, y)$ of size $N \times N$ goes through the same steps as the image $I_H(x, y)$ cited before to obtain the matrix ES_W . With the exception of step 1, we compute the QCMs of image $I_W(x, y)$ using Eq. (24) up to order N , and in step 2, the image $I_W(x, y)$ is subjected to a single decomposition $1 - DWT$.

Step 6: Calculate the integrated singular value ES_{HW} by using a scaling factor θ .

$$ES_{HW} = ES_H + \theta \cdot ES_W \quad (31)$$

The final stage of the watermarking process involves the reconstruction of the watermarked image. This is a critical step to ensure that the watermark is correctly embedded in the image and can be reliably extracted later. The reconstruction process follows a series of carefully designed steps, as depicted in Fig. 6.

Watermark extraction process

The phase of watermark extraction uses the watermarked host image $I_{HW}(x, y)$ of size $M \times M$ as input as long as the extracted watermark $I_W^*(x, y)$ of size $N \times N$ is the output of this phase. This process is illustrated in Fig. 8. We describe the extraction process in the following sequence of steps (the images used in this Fig. 8 are selected from database Ref.⁴² and website Ref.⁴³).

Step 1: Compute the MCQs of the input image using Eq. (13) up to order M for image $I_{HW}(x, y)$

Step 2: Use the $k - DWT$ transformation to decompose the $I_{HW}(x, y)$ image into four equals $LL_{HWk}, LH_{HWk}, HL_{HWk}$ and HH_{HWk} subbands.

Step 3: Use QR to decompose LL_{HWk} into Q_{HW} and R_{HW} .

Step 4: Use SVD decomposition, to decompose R_{HW} into three matrices U_{HW}, S_{HW} and V_{HW} .

Step 5: Encrypt S_{HW} using 2D-FrMHM to acquire the $\hat{E}S_{HW}$ matrix.

Step 6: Utilize the scaling factor θ to compute the singular value $\hat{E}S_{HW}$.

$$E\hat{S}_W = \frac{\hat{E}S_{HW} - ES_{HW}}{\theta} \quad (32)$$

Step 7: Decrypt the $\hat{E}S_W$ using 2D-FrMHM to obtain the $\hat{S}_W$ matrix.

Step 8: Apply the inverse of the SVD transformation to obtain the matrix $\hat{R}_W$.

Step 9: Apply inverse QR decomposition to recover the $\hat{L}_{W1}$ matrix, followed by the inverse operation of the DWT transformation.

Step 10: Apply the inverse operation of the QCM to reconstruct watermark $I_W^*(x, y)$ with size $N \times N$.

After presenting in detail the operation of the watermarking system, which generates color images incorporating watermarks from the original images and watermarks, the next section looks at the use of AOA optimization to discover the optimum scaling factor.

Scale factor optimization via AOA

Preliminaries of the AOA algorithm

The AOA algorithm is based on the four fundamental arithmetic operators ($+$, $-$, $\times$, and $/$). The optimization process of this algorithm has two key steps: an inspection phase and a manipulation phase. Figure 9 presents an overview of the two phases and their roles^{44,45}.

In the following, we will give a more detailed overview of the AOA. First, we start with the initialization step, in which a set of candidate solutions is randomly created $X = [x_{1,1}; x_{2,1}; \dots; x_{N,n}]$. In addition, Eq. (34) is chosen to play the accelerating function.

Before starting the work process, the AOA must determine the search phase, either inspection or manipulation. The Math Optimizer Accelerated (MOA) function represents a coefficient calculated according to Eq. (33), which is then used in the search stages. Where C_{iter} and M_{iter} denote the current iteration and the maximum number of iterations.

$$MOA(C_{iter}) = MOA_{\min} + C_{iter} \times \left(\frac{MOA_{\max} - MOA_{\min}}{M_{iter}} \right); C_{iter} \in [1, M_{iter}] \quad (33)$$

The inspection phase within AOA involves multiple convergent iterations aimed at thoroughly exploring the entire search space to ensure broad coverage. To prevent convergence into local solutions, AOA leverages arithmetic operators (refer to Eq. 37) in conjunction with the optimization probability function (MOP) (see Eq. 35)⁴⁵.

$$x_{i,j}(C_{iter} + 1) = \begin{cases} best(x_j)/(MOP + \varepsilon) \times ((UB_j - LB_j) \times \mu + LB_j), & r_2 < 0.5 \\ best(x_j) \times MOP \times ((UB_j - LB_j) \times \mu + LB_j), & \text{otherwise} \end{cases} \quad (34)$$

where ε , μ and MOP denote an integer, the control parameter for adjusting the search process and the function of the optimization probability, respectively.

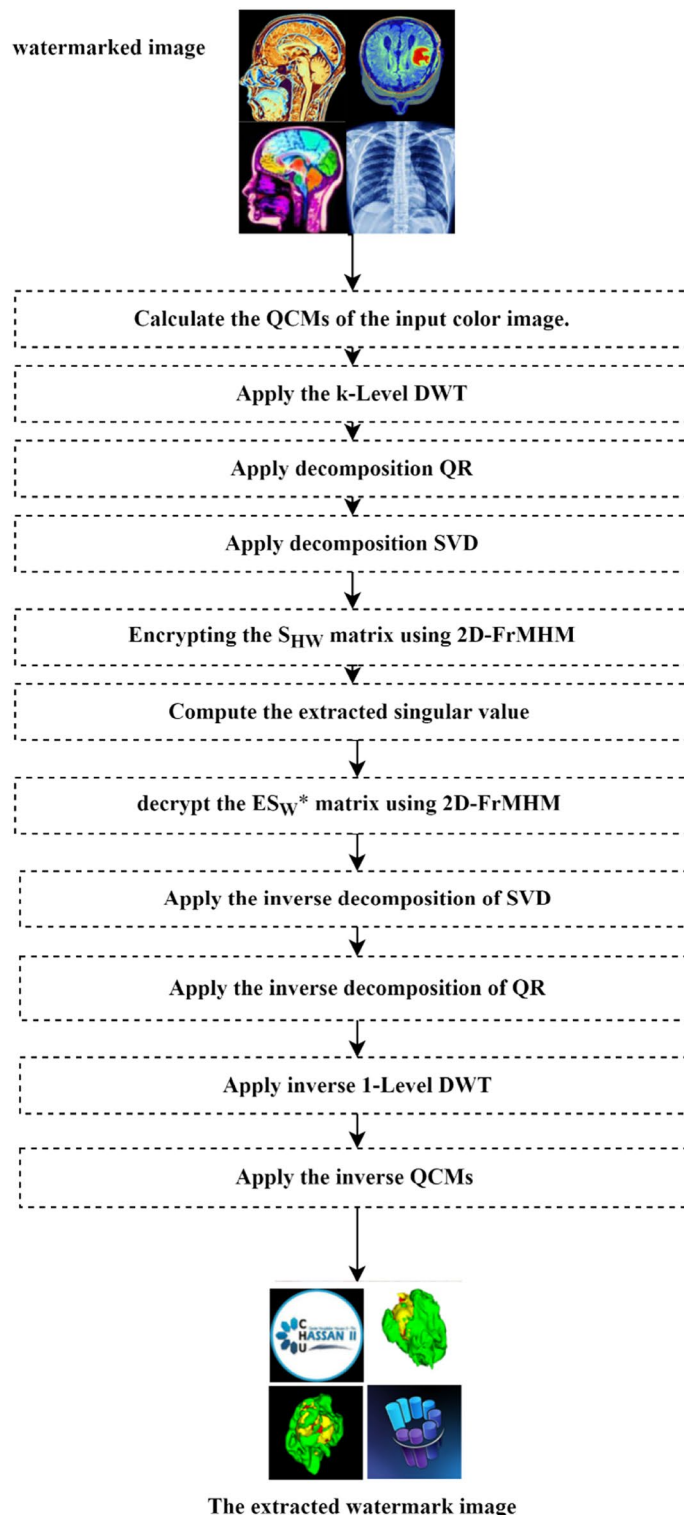


Figure 8. Watermark extraction procedure.

$$MOP(C_{iter}) = 1 - \frac{C_{iter}^{1/\alpha}}{M_{iter}^{1/\alpha}}; \quad C_{iter} \in [1, M_{iter}] \quad (35)$$

During the manipulation phase, AOA enables precise convergence to attain an enhanced solution following the inspection phase. This phase primarily relies on arithmetic operators, specifically subtraction (-) and addition (+), as defined in Eq. (36), in combination with the MOP as described in Eq. (35)⁴⁵.

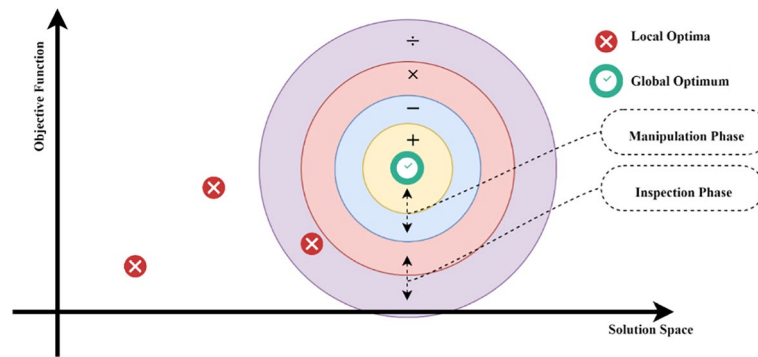


Figure 9. Two phases of inspection and manipulation of the AOA algorithm.

$$x_{i,j}(C_{iter} + 1) = \begin{cases} best(x_j) - (MOP + \varepsilon) \times ((UB_j - LB_j) \times \mu + LB_j), & r_3 < 0.5 \\ best(x_j) + MOP \times ((UB_j - LB_j) \times \mu + LB_j), & \text{otherwise} \end{cases} \quad (36)$$

Scale factor optimization

The watermark insertion and extraction process consists of several successive steps: calculation of the QCMs of the input color image, application of the discrete wavelet transform, QR decomposition, SVD decomposition and encryption via 2D-FrMHM. These steps are used to generate watermarked color images, as illustrated in Figs. 7 and 8. This process is highly dependent on a scaling factor. To find a suitable factor, we propose to use an efficient optimization algorithm. This optimization algorithm is inserted after step 6, which involves calculating the integrated singular value, as described in “Proposed watermark scheme for color images” of the proposed watermarking scheme for color images (Fig. 10).

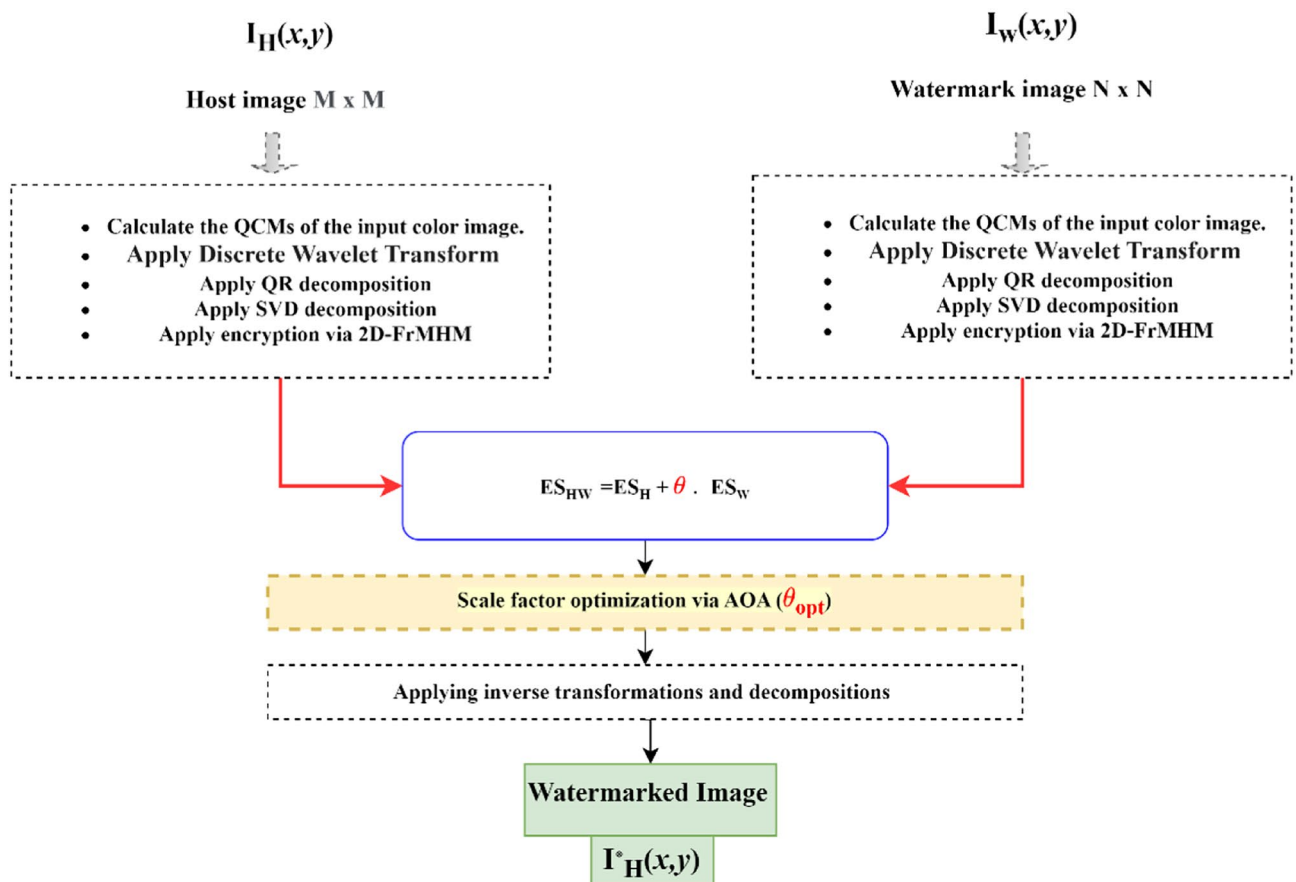


Figure 10. Integrating the AOA into the watermark insertion process.

It should be noted that the scaling factor θ presented in “Improved reversible watermarking scheme”, more precisely Eq. (31), varies according to the host image $I_H(x, y)$ and watermark $I_W(x, y)$, meaning that different watermarks require different scaling factors, even if they are all embedded in the same host image. This paper opts for the use of AOA to improve the reliability and robustness of our new system. The proposed process for selecting optimal values of the scaling factor using AOA aims to solve the challenge of the trade-off between invisibility and robustness. This algorithm is summarized in Algorithm 2. In addition, standard performance metrics such as PSNR, NC, and SSIM are also employed to assess the visibility and reliability of the proposed system.

We apply these steps to develop an objective function, which we will henceforth refer to as FO_{θ}^{opt} . This function will serve as the basis for our subsequent work.

$$MSE(I_H, I_H^*) = \frac{1}{M^2} \sum_{i=1}^M \sum_{j=1}^M (I_{H_{ij}} - I_{H_{ij}}^*)^2 \quad (37)$$

$$PSNR(I_H, I_H^*) = 10 \lg \frac{I_{MAX}^2}{MSE} \quad (38)$$

$$NC(I_W, I_W^*) = \frac{\sum_{i=1}^N \sum_{j=1}^N I_{W_{ij}} I_{W_{ij}}^*}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N I_{W_{ij}}^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^N I_{W_{ij}}^{2*}}} \quad (39)$$

$$SSIM(I_H, I_H^*) = \frac{\mu_{I_H} \mu_{I_H^*} + d_1}{\mu_{I_H}^2 + \mu_{I_H^*}^2 + d_1} \cdot \frac{\sigma_{I_H I_H^*} + d_2}{\sigma_{I_H}^2 + \sigma_{I_H^*}^2 + d_2} \quad (40)$$

where $\sigma_{I_H}^2$ and $\sigma_{I_H^*}^2$ are the variances of I_H and I_H^* . $\sigma_{I_H I_H^*}$ is the covariance of I_H and I_H^* . d_1 and d_2 are two variables that are used to stabilize the division with a low denominator, and FO_{θ}^{opt} is defined to optimize the scaling factor, which is given by the following equation.

$$FO_{\theta}^{opti} = \frac{PSNR(I_H, I_H^*)}{\lambda} + SSIM(I_H, I_H^*) + NC(I_W, I_W^*) \quad (41)$$

By applying the formula $(PSNR/\lambda)$, the PSNR undergoes a normalization that takes into account the weighting factor λ . Typical PSNR values are in the range of 1 to 70 dB. Therefore, if the $PSNR/\lambda$ ratio is equal to or greater than 1, this indicates that the watermark is sufficiently discrete to be deemed acceptable. On the other hand, if this ratio is less than 1, the watermark is detectable and therefore considered unacceptable.

Algorithm 2 summarizes the idea of optimizing the scaling factor θ by seeking to maximize the objective function FO_{θ}^{opti} . This step is based on the AOA algorithm: First, we select the host $I_H(x, y)$ image and watermark $I_W(x, y)$, taking into account the initial parameters of the AOA algorithm and the FO_{θ}^{opti} . Next, the algorithm randomly generates a set of initial solutions. These solutions are evaluated using the FO_{θ}^{opti} . Next, the algorithm updates the scaling factor θ using the exploration and exploitation phases of the AOA algorithm, and we evaluate the value of the FO_{θ}^{opti} . This step is repeated iteratively until the maximum number of iterations is reached (M_{iter}). Finally, the output of this optimization generates the optimal values of the scaling factor θ_{opt} and the watermarked image I_H^* .

Inputs: I_H , C_{iter} , M_{iter} , objective function FO_{θ}^{opti}

Output: Optimal scaling factor θ_{opt} , watermarked image I_H^*

- $n = 50$ (The population of AOA size)
- $M_{iter} = 100$ (Maximum iterations number)
- $m = 1$ (set number of design variable)
- $\mathbf{X}$ (Initialize $\mathbf{X}$ the candidate solution set of the AOA)
- $\mathbf{Lb}$ = (The minimum of design variable)
- $\mathbf{Ub}$ = (The maximum of design variable)
- Initialize α and μ of AOA
- The MOA and MOP values are calculated using Eq (33) and Eq (35).
- Evaluate the objective function FO_{θ}^{opti} given by Eq. (41).
- Identify the best solution for the population.

For $i=l$ to n do**For $j=1$ to m do**
$$r1, r2, \text{ and } r3 = rand(0,1)$$

///{r1, r2, and r3 are random number }

if $r1 > MOA$

if $r2 > 0.5$ (*Exploration Phase*)

$$x_{i,j} = best(x_j) / (MOP + \varepsilon) \times ((UB_j - LB_j) \times \mu + LB_j)$$

else

$$x_{i,j} = best(x_j) \times MOP \times ((UB_j - LB_j) \times \mu + LB_j)$$

End if

elseif $r > 3$ (*Exploitation Phase*)

$$x_{i,j} = best(x_j) - (MOP + \varepsilon) \times ((UB_j - LB_j) \times \mu + LB_j)$$

else

$$x_{i,j} = best(x_i) + MOP \times ((UB_i - LB_i) \times \mu + LB_i)$$

End if**End for**

$$M_{iter} = M_{iter} + 1$$

End for

Algorithm 2: Scale factor optimization steps.

Simulations and findings

In this section, we evaluated the efficiency of the proposed watermarking method, which is based on quaternion moments, wavelet transforms, algebraic decompositions, and the modified Henon map. To enhance clarity, this section is divided into three subsections.

- The first subsection focuses on evaluating the robustness of the encryption with the modified Henon map. It includes an in-depth security analysis, a detailed histogram study, a correlation investigation as well as an entropy analysis.
- The second subsection examines the performance of the proposed digital watermarking system. This part of the analysis covers the impact of the choice of scale factor and carries out a careful analysis of the invisibility and robustness of digital watermarking.
- The third subsection provides a detailed comparison with similar works. This comparison highlights key differences between our approach and existing approaches, as well as the specific advantages of our method.

Additionally, we consider NC along with SSIM and PSNR to evaluate the robustness aspect of this innovative watermarking scheme. A summary of these and other metrics can be found in Fig. 11 for reference^{1,2,46–49}.

Encryption process using 2D-FrMHM

Security analysis

The security key (KEY) produced by 2D-FrMHM is formed by the concatenation of the keys generated in step 5 of the watermark insertion process $KEY = \{\alpha, \beta, x(0), y(0), x^*(0), y^*(0), \phi_1, \phi_2, \phi_3, \phi_4, v\}$.

The following scenario aims to evaluate key sensitivity in the following steps: Firstly, the original image shown in Fig. 12a undergoes an encryption process using the "KEY" security key, thereby generating the encrypted RGB

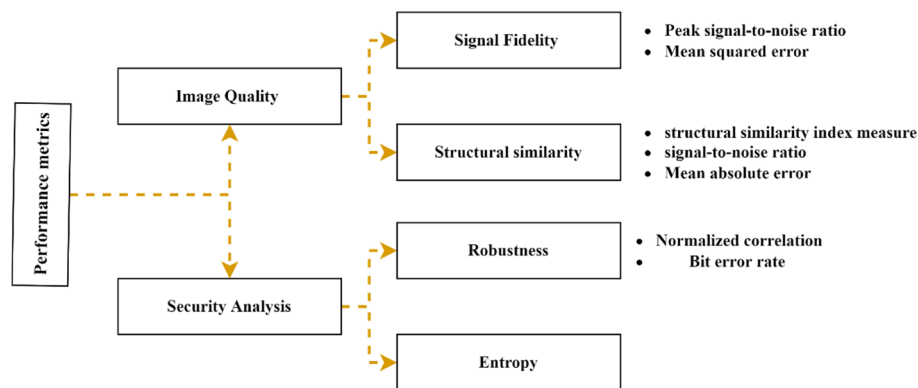


Figure 11. Digital watermarking metrics.

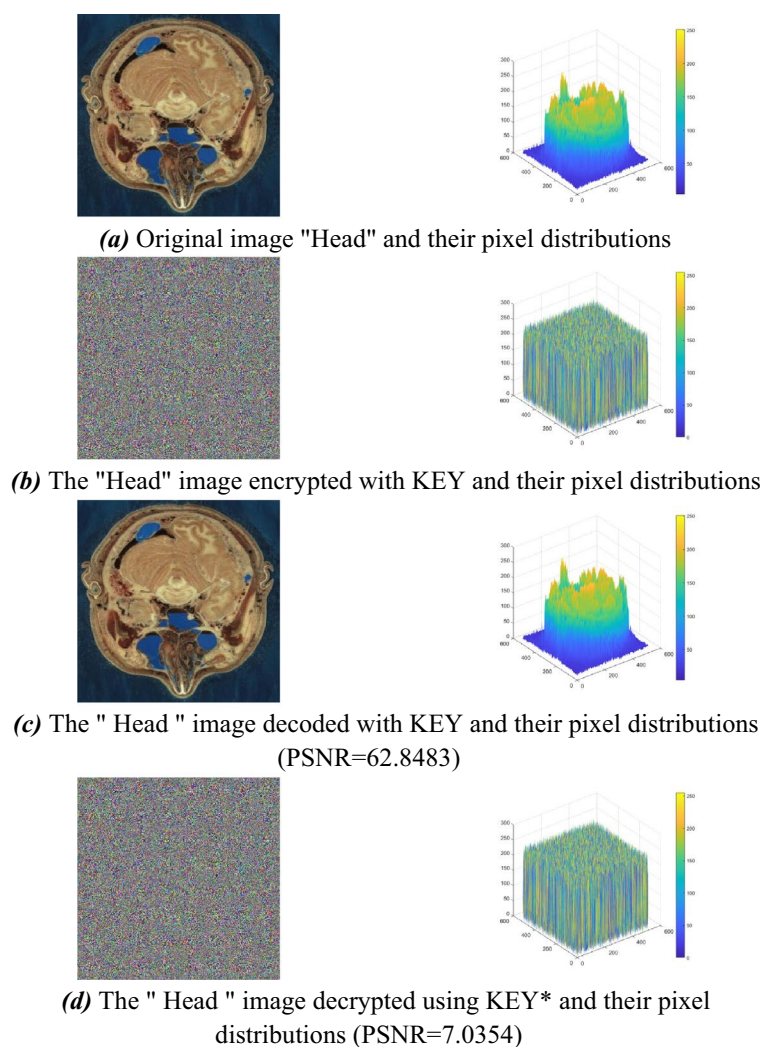


Figure 12. Key sensitivity with a modification of 10^{-15}

image⁴² shown in Fig. 12b. Figure 12c depicts the image decrypted by the correct key. Next, the "KEY" security key undergoes a minor modification, equivalent to a change in order by 10^{-15} , thus becoming "KEY*." The original encrypted image is then decrypted using the modified "KEY*" key. The conclusions of this evaluation reveal that the proposed system is highly sensitive to variations in the security key, particularly evident in PSNR values that do not exceed 10 dB, as illustrated in Fig. 12d.

Histogram analysis

Optimal encryption should generate encrypted images with as uniform a histogram as possible⁵⁰. As illustrated in Fig. 13, the histograms of the three channels of the encrypted image⁴² (R, G and B) show a horizontal distribution. This demonstrates the effectiveness of the proposed 2D-FrMHM in terms of resistance to statistical attacks.

Correlation and entropy analysis

Correlation analysis is a well-established approach to evaluating the relationships between pixels in an image⁵¹. It quantifies the statistical dependence between the brightness or color values of different pixels. This analysis is crucial in various fields, including computer vision, image processing and statistics. To measure the correlation between each pair of pixels, we use the following formula²³.

$$r(J_1, J_2) = \frac{\text{Cov}(J_1, J_2)}{\sigma(J_1)\sigma(J_2)} \quad (42)$$

when

$$\begin{cases} r(J_1, J_2) = -1 \text{ or } +1 \\ r(J_1, J_2) = 0 \end{cases} \quad (43)$$

Using point maps to visually represent the correlation between pixels before and after encryption is an effective way of assessing the impact of the encryption process on the image. This method makes it possible to highlight changes in the spatial distribution of pixel values and determine whether encryption has succeeded in disrupting the correlation between pixels in the original image. Specifically, in Fig. 14, the dot maps show the correlation coefficients between adjacent pixels in the three-color channels (R, G, and B) of the image. Prior to encryption, when the image is still unaltered, neighboring pixels can be expected to show strong correlation, resulting in coherent patterns on the dot maps.

To reinforce this observation, we proceeded to calculate the correlation coefficients on another 512×512-pixel medical image⁴² using different chaotic maps reported in previous work (see Table 3). This comparative analysis highlights that the correlation coefficients associated with the encrypted osteochondroma image tend towards zero, indicating extremely low correlation.

The entropy analysis, as presented in Table 4, highlighted that all three channels of the encrypted image (Red, Green and Blue) exhibit information entropy very close to the theoretical maximum value of 8. These results conclusively confirm that the 2D-FrMHM model is highly effective in defending against attacks that attempt to take advantage of the information entropy present in the image. This observation is of great importance, as it demonstrates the robustness of the 2D-FrMHM model in the face of attack attempts specifically aimed at disrupting the entropy of information within the image. Entropy, being a crucial indicator of data complexity and disorganization, would play a key role in preserving the security and confidentiality of encrypted images.

Image watermark

Effects of the choice of the scaling factor

To assess the influence of the scale factor on the process of incorporating and extracting color watermarks, we used two separate images. The first comes from the database "The Visible Human Project" and has a resolution of 512×512⁴². The second represents the logo of the Hassan II Hospital in Fez⁴³ and has a resolution of 128×128,

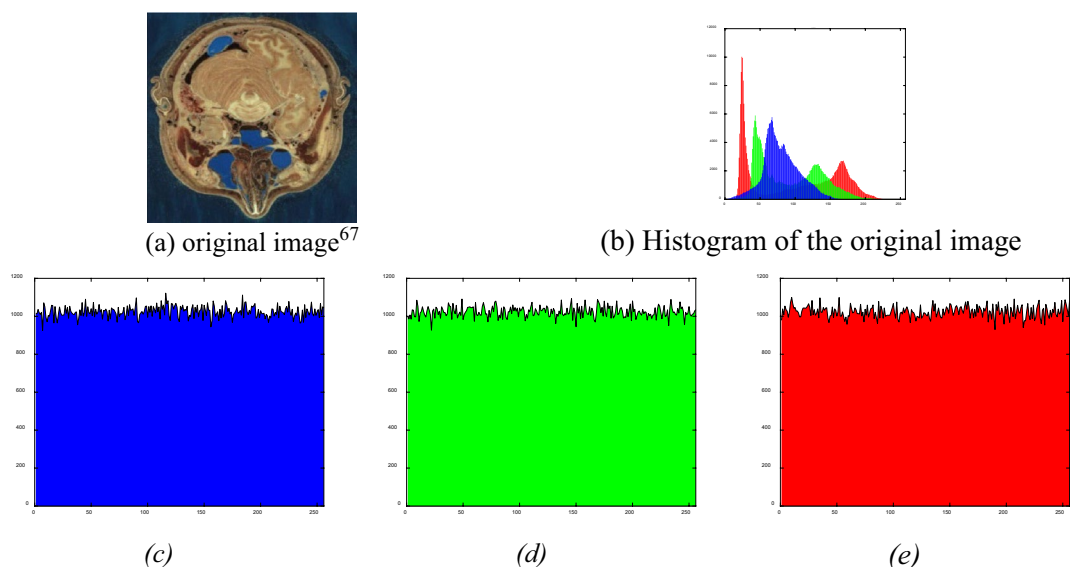


Figure 13. Histogram analysis.

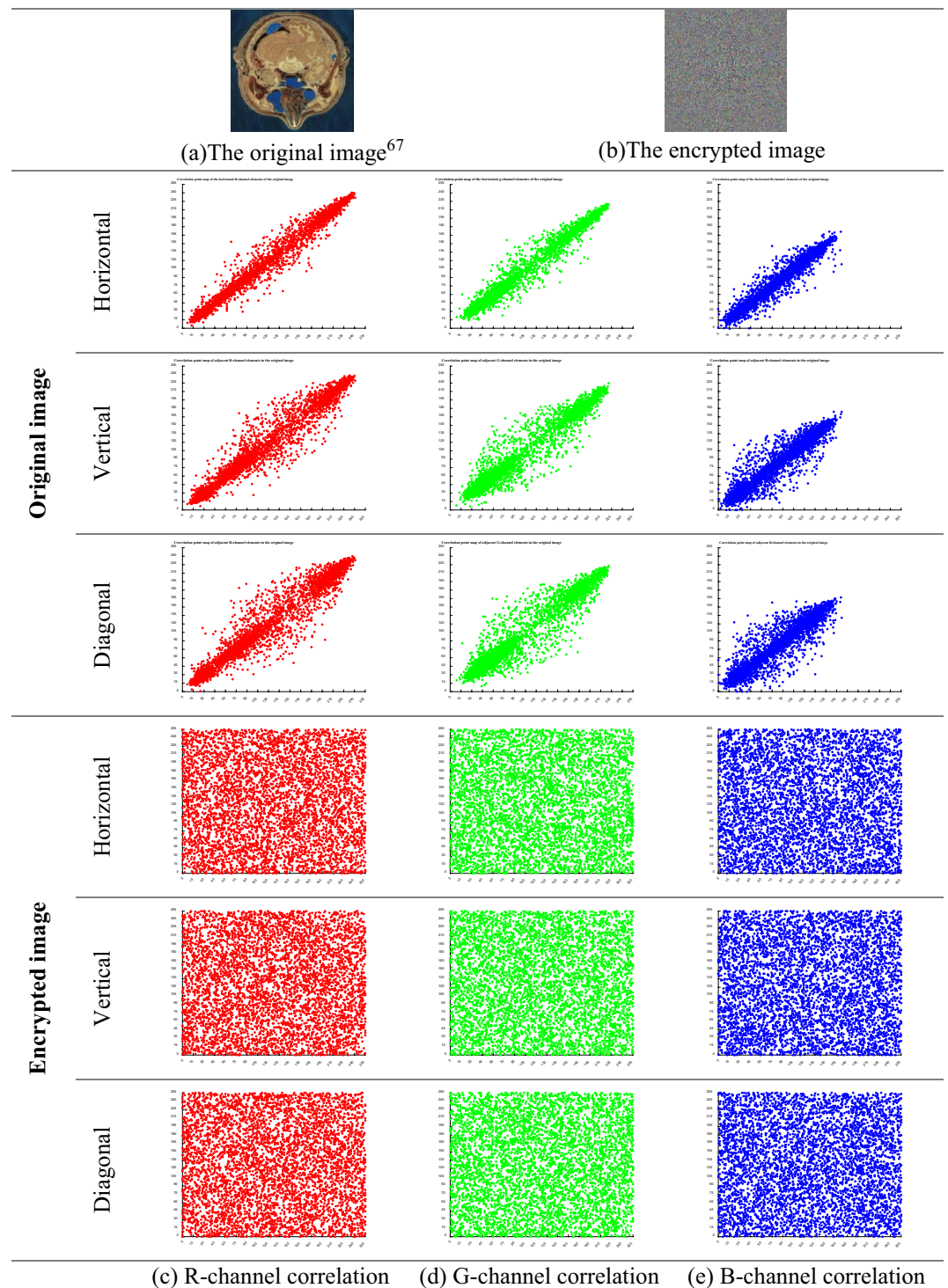


Figure 14. Correlation point map.

as shown in Fig. 15. The incorporation and extraction phases reveal that the scaling factor, denoted θ , exerts a significant influence on the quality of the filtered image as well as on the extracted watermark. In this experiment, we systematically modified the value of θ , ranging from 0.01 to 1. The optimum value is the one that achieves the best balance between imperceptibility and robustness. It is important to note that the choice of scale factor depends on both the host image ($I_H(x, y)$) and the watermark ($I_W(x, y)$) used. Consequently, different watermark images require different scaling factors, even if they are inserted in the same host image.

In light of these results, we chose to adopt the AOA algorithm⁴⁵ in conjunction with the objective function (FO_{θ}^{opt}) to solve the θ parameter challenge. Table 5 provides a comparison with other algorithms, including

			
Algorithm	Horizontal	Vertical	Diagonal
Ref. ⁵²	− 0.02713	0.02974	0.02543
Ref. ⁵³	0.06955	0.04805	0.02242
Ref. ⁵⁴	− 0.00296	0.00135	− 0.00261
Ref. ⁵⁵	0.00342	0.00538	0.00445
Ref. ⁵⁰	0.00237	− 0.00201	0.00128
Proposed	0.0012	− 0.0010	0.0024

Table 3. Correlation values.

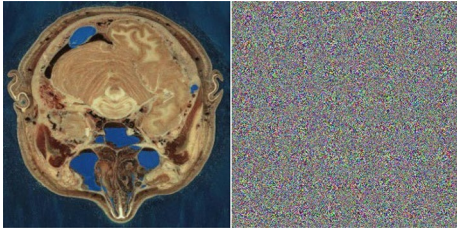
				
Image de test	Algorithm	Red	Green	Blue
Head 512 × 512	Ref. ⁵⁶	7.9964	7.9970	7.9957
	Ref. ⁵⁷	7.9957	7.9961	7.9959
	Ref. ⁵⁵	7.9954	7.9962	7.9955
	Proposed	7.9995	7.9992	7.9991

Table 4. The entropy values found by 2D-FrMHM and other static systems.

particle swarm optimization⁵⁸ (PSO), gray wolf optimization⁵⁹ (GWO), and artificial bee colony optimization⁶⁰ (ABC). Performance, assessed using standard metrics such as PSNR, NC, and SSIM, testifies to the superiority of our algorithm. Note that the four selected algorithms adopt a maximum iteration of 200. This means that each algorithm has a fixed limit of 200 execution cycles to attempt to reach an optimal solution. To ensure reliable results, each algorithm is run independently 15 times. This minimizes the effect of random variation and provides a representative average of each algorithm’s performance. The results recorded during these multiple runs are then compiled and presented in Table 5.

Invisibility and robustness analysis

In this evaluation, we examined how the size of the color watermark affects the embedding and extraction steps⁶¹. To illustrate this process, Fig. 16 shows watermarked host images, together with the corresponding extracted watermarks⁴², with dimensions of 256 × 256 and 128 × 128 pixels (the images used in this Fig. 16 are selected from database Ref.⁴² and website Ref.⁴³).

To carry out this evaluation, this section highlights a real 512 × 512 pixel medical image⁴². As can be seen in Fig. 16, the proposed digital watermarking system achieved its objectives, with results clearly defined by PSNR values above 70.00 and SSIM values above 0.99. The NC of the extracted watermarks all shows a value of 1.0000 (no alterations were made to the watermarked host images). This indicates the excellent visibility of the watermarking method. In summary, the proposed watermarking scheme can satisfy the prerequisites for invisible watermarks. In addition, the use of a watermark of size 128 × 128 produces superior results to those obtained by using a watermark of size 256 × 256.

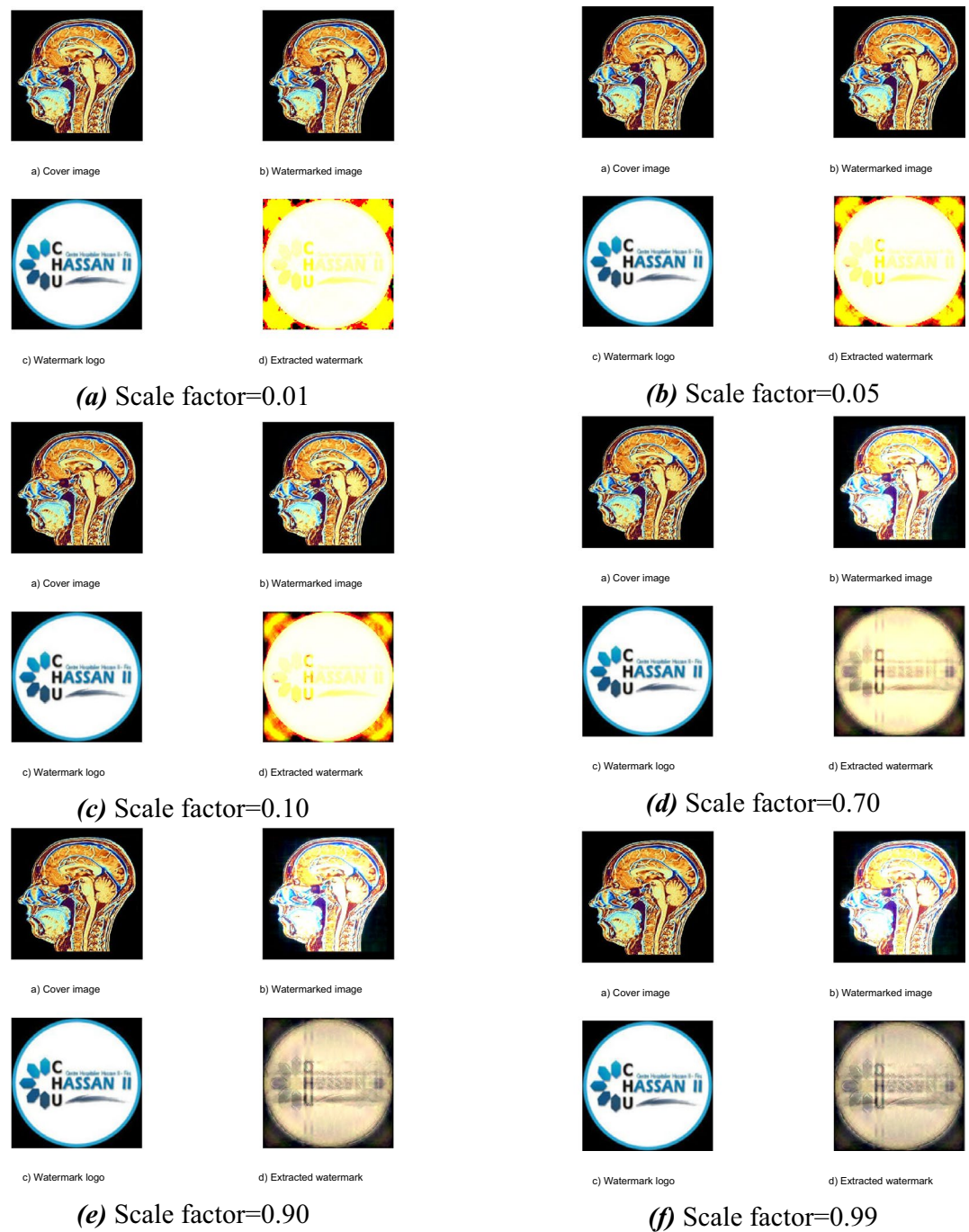


Figure 15. Watermarked image and extracted watermark using different scale factor choices.

Algorithm	PSNR (dB)	NC	SSIM
AOA	77.84	0.9979	0.9965
PSO	53.94	0.8904	0.9823
GWO	57.87	0.8756	0.9783
ABC	49.32	0.8570	0.9621

Table 5. Optimization results.

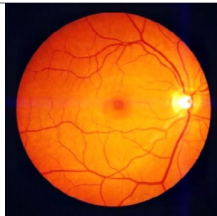
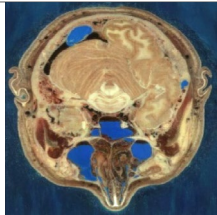
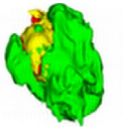
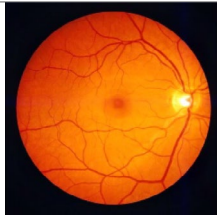
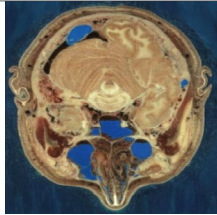
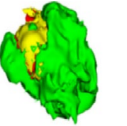
Watermarked image	Extracted watermark	PSNR	SSIM	NC
	 256×256	72.45	0.9934	1.000
	 256×256	71.34	0.9927	1.000
	 128×128	77.54	0.99999	1.000
	 128×128	76.86	0.9998	1.000

Figure 16. Extracted watermarks of different dimensions from a watermarked image.

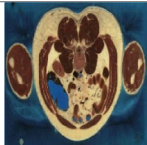
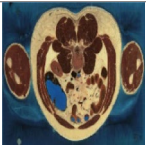
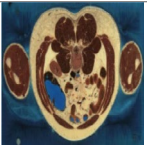
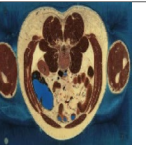
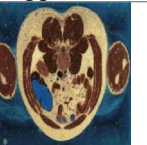
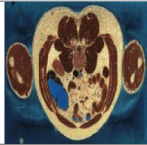
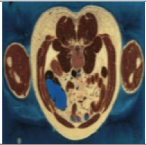
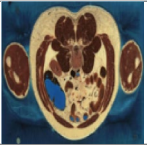
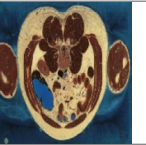
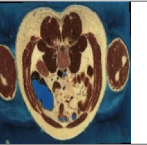
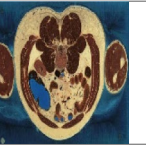
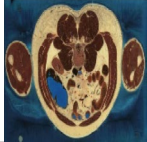
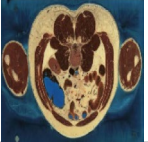
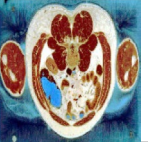
Wiener filter	Median filter	Gaussian filter	Average filter	Salt and Pepper noise	Gaussian noise
					
Speckle noise	Motion blur	Rescaling 0.25	Rescaling 4	Rotation	Sharpening
					
JPEG compression	JPEG 2000 compression		HE		
					

Figure 17. Types of attacks on watermarked images.

To assess the robustness of the proposed watermarking system, first, as shown in Fig. 17, we subjected photographs that were previously watermarked with color watermarks of sizes 128×128 and 256×256 to various attacks (see Table 6). Next, we extracted the watermark and calculated the normalization coefficient (NC) values. Figure 18 is an important illustration of the robustness of the watermarking system we developed. It shows the watermarks that we were able to recover after subjecting the watermarked images to various filtering attacks, such as scaling, applying filters, adding noise, and other similar attacks. We carried out these tests on two sets of watermarks, one of size 128×128 pixels and the other of size 256×256 pixels. Table 7 contains the PSNR, NC

Type of filter	Wiener	Size 3×3
	Median	
	Gaussian	
Type of noise	Gaussian	$V = 0.001$
	salt and pepper	0.001
Type of compression	JPEG	QF = 40
	JPEG 2000	CR = 8
Type of rescaling	Rescaling-1	$\times 0.25$
	Rescaling-2	$\times 4$
Type of rotation	Angle	Degree = 2
Sharpening	1-Sharpening	0.2

Table 6. Attacks used and related parameters.

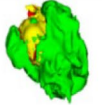
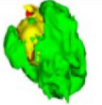
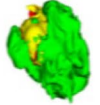
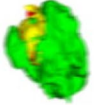
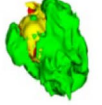
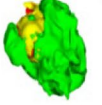
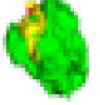
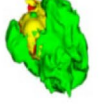
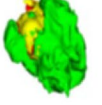
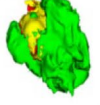
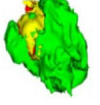
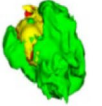
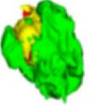
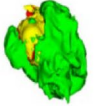
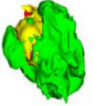
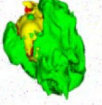
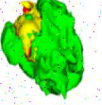
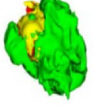
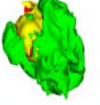
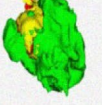
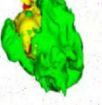
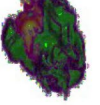
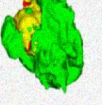
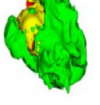
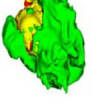
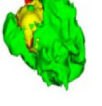
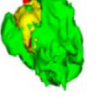
Attacks	256×256	128×128	Attacks	256×256	128×128
Wiener filter			Motion blur		
Median filter			Rescaling 0.25		
Gaussian filter			Rotation		
Average filter			JPEG compression		
Salt and Pepper noise			JPEG 2000 compression		
Gaussian noise			HE		
Speckle noise			Sharpening		
Rescaling 4					

Figure 18.. Extracted the watermark 128×128 and 256×256 .

Attacks	256 × 256	128 × 128	Attacks	256 × 256	128 × 128
Wiener filter attacks	NC = 0.9995	NC = 0.9990	Motion blur	NC = 0.8945	NC = 0.8346
	SSIM = 0.9945	SSIM = 0.9952		SSIM = 0.9954	SSIM = 0.9961
	PSNR = 54.53	PSNR = 46.73		PSNR = 0.4367	PSNR = 48.53
Median filter	NC = 0.9978	NC = 0.9968	Rescaling 0.25	NC = 97.45	NC = 0.8543
	SSIM = 0.9976	SSIM = 0.9980		SSIM = 0.9953	SSIM = 0.9967
	PSNR = 51.63	PSNR = 56.29		PSNR = 51.61	PSNR = 53.63
Gaussian filter	NC = 0.9940	NC = 0.9966	Rotation	NC = 0.9963	NC = 0.9935
	SSIM = 0.9974	SSIM = 0.9991		SSIM = 0.9934	SSIM = 0.9924
	PSNR = 51.93	PSNR = 56.47		PSNR = 42.32	PSNR = 46.63
Average filter	NC = 0.9999	NC = 0.9999	JPEG compression	NC = 0.9999	NC = 0.9995
	SSIM = 0.9964	SSIM = 0.9970		SSIM = 0.9941	SSIM = 0.9959
	PSNR = 49.36	PSNR = 50.56		PSNR = 53.67	PSNR = 57.49
Salt and pepper noise	NC = 0.9934	NC = 0.9921	JPEG 2000 compression	NC = 0.9998	NC = 0.9984
	SSIM = 0.9958	SSIM = 0.9962		SSIM = 0.9986	SSIM = 0.9932
	PSNR = 49.63	PSNR = 50.73		PSNR = 43.24	PSNR = 48.73
Gaussian noise	NC = 0.9748	NC = 0.9895	HE	NC = 68.59	NC = 0.6841
	SSIM = 0.9935	SSIM = 0.9956		SSIM = 0.8675	SSIM = 0.8731
	PSNR = 48.63	PSNR = 56.70		PSNR = 16.23	PSNR = 17.35
Speckle noise	NC = 0.9746	NC = 0.9676	Sharpening	NC = 0.9998	NC = 0.9975
	SSIM = 0.9963	SSIM = 0.9972		SSIM = 0.9982	SSIM = 0.9985
	PSNR = 39.43	PSNR = 40.69		PSNR = 53.76	PSNR = 54.35

Table 7. PSNR and SSIM of watermarked images, the NC of watermarks.

and SSIM measurements which provide a comprehensive assessment of the quality and fidelity, whether of the watermarked image compared to the original or of the watermark before its insertion and after its extraction. To maintain consistency with Eq. (41), which defines the objective function, we assigned the PSNR and SSIM measurements to the watermarked images, while the NC is used to evaluate the watermark. The results shown in Table 7 indicate that our watermarking system is able to recover watermarks reliably even after being subjected to filtering attacks. This confirms the robustness of the system, essential to guarantee the security and integrity of watermarks in real-world conditions where images may be exposed to different types of alterations.

In summary, the use of a variety of watermarks has emphasized the robustness of our digital watermark. After performing several attacks on the watermarked image and determining the NC value of each attack using two watermarks, the first of size 128×128 and the second of size 256×256 . Figure 19 illustrates how the average NC value varied depending on the attack used, including the filter attack, noise attack, compression attack, scaling

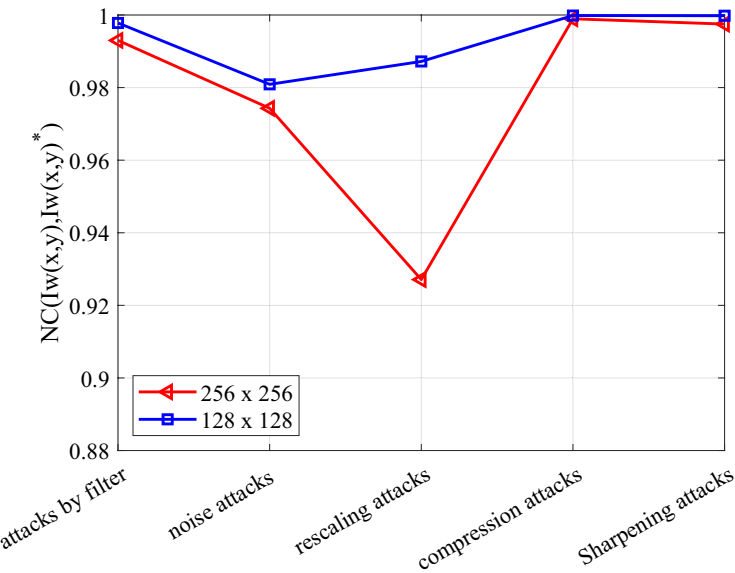


Figure 19. Average NC values after the application of certain attacks.

attack, and sharpening attack. The red curve represents this variation when using a 256×256 size watermark, while the blue curve illustrates this variation when using a 128×128 size watermark. The results shown in this figure show that, when a small watermark is used, our method works well.

Table 8 shows a comparative study of the robustness of our method with other works that are based on metaheuristic algorithms, including an ABC-based watermark, a PSO-GWO based watermark, and an ABC-based watermark. From the results shown in Table 8, we can see that the proposed method provides a high NC compared to the other methods under the different attacks. It is important to note that the attack parameters we examined earlier were static, i.e., fixed and pre-set. However, to get a more complete and realistic view of the robustness of our watermarking system, it is also essential to take into account dynamic parameters, which can vary depending on the situation or environment.

In order to better understand the impact of dynamic parameter choices when applying attacks, we conducted tests taking these parameter variations into consideration. The results of these tests are shown in Fig. 20. This approach enables us to demonstrate the ability of our system to maintain its robustness even when attack parameters vary.

Comparison with similar work and discussion of results

To guarantee the credibility and validity of our results, we have undertaken an essential step to validate and authenticate our method. In this subsection, our system, based on a combination of DWT, QR, SVD, and the 2D-Henon map, is subjected to a detailed comparison with several other related methods. This comparison is based on a set of crucial features, as shown in Table 9. In this comparative analysis, we take into account a series of important properties, each of which has a significant impact on overall performance.

As the table clearly illustrates, our proposed approach proves extremely effective in comparison with other methods based on standard metrics^{64,65}. These remarkable results can be attributed to several key factors that distinguish our approach. Firstly, the use of discrete orthogonal moments in their quaternion form. QCMs are particularly effective for representing images with low information redundancy, while preserving the visual quality of the images used in the proposed watermarking system. What's more, our system benefits from scale factor optimization via the AOA optimization algorithm, which guaranteed precise scale factor adjustment for each specific host image and watermark. By combining these two elements—the use of QCM and scale factor optimization via AOA—our system offers superior performance in terms of image quality and watermark detection capability. Thanks to this combination of techniques, we are able to achieve outstanding results, reinforcing the effectiveness and reliability of our watermarking method.

Conclusion

In this work, we introduced a novel watermarking system designed to guarantee the robust integrity of color images. Our method is founded on the use of moment and wavelet transformations, algebraic decompositions, and chaotic systems. As a first step, we have extended the scope of classical Charlier moments by adapting them to QCM through the exploitation of quaternion algebra. This first phase of our system enabled us to perform the DWT without requiring color image decomposition while minimizing the computational load at each stage of the process. Subsequently, we performed a decomposition of the resulting matrix generated by the DWT using QR decomposition and SVD. Then, to enhance the safety and robustness of our system, we used a modified version of Henon's 2D chaotic map, characterized by extended parameters compared to the classical version. Finally, to optimize watermark insertion, we employed the arithmetic optimization algorithm, enabling dynamic and adaptive estimation of the scaling factor. This overall approach is designed to guarantee the security, reliability, and capacity of our watermarking system while maintaining the excellent invisibility of watermarks inserted in color images. Experimental results show that our approach outperforms recent color image processing methods in terms of security, storage capacity, and resistance to various attacks while maintaining high invisibility. In the future, we intend to put our watermarking system into practice using programmable electronic boards such as Arduino and Raspberry Pi. This is intended to overcome the limitations of our current system, notably the high computation time involved in using a meta-heuristic.

Attacks	Parameters	Ref. ⁶²	Ref. ⁶³	Ref. ¹⁴	Proposed method
Median filter	3×3	0.9637	0.9783	0.9960	0.9988
Gaussian filter	3×3	0.9676	0.9785	0.9957	0.9966
Gaussian noise	$V = 0.001$	0.9843	0.8020	0.9971	0.9632
Salt and Pepper noise	0.001	0.9975	0.9790	0.9980	0.9896
JPEG compression	QF = 40	0.9856	0.9810	0.9965	0.9996
JPEG 2000 compression	CR = 8	0.9878	0.9860	0.9970	0.9998
Rescaling1	$\times 0.25$	0.9963	0.9912	0.9903	0.8553
Rescaling 2	$\times 4$	0.9934	0.9989	0.9957	0.9989
1-Sharpener	0.2	0.9763	0 0.9239	0 0.9836	0.9975

Table 8. The NC values found compared with different methods.

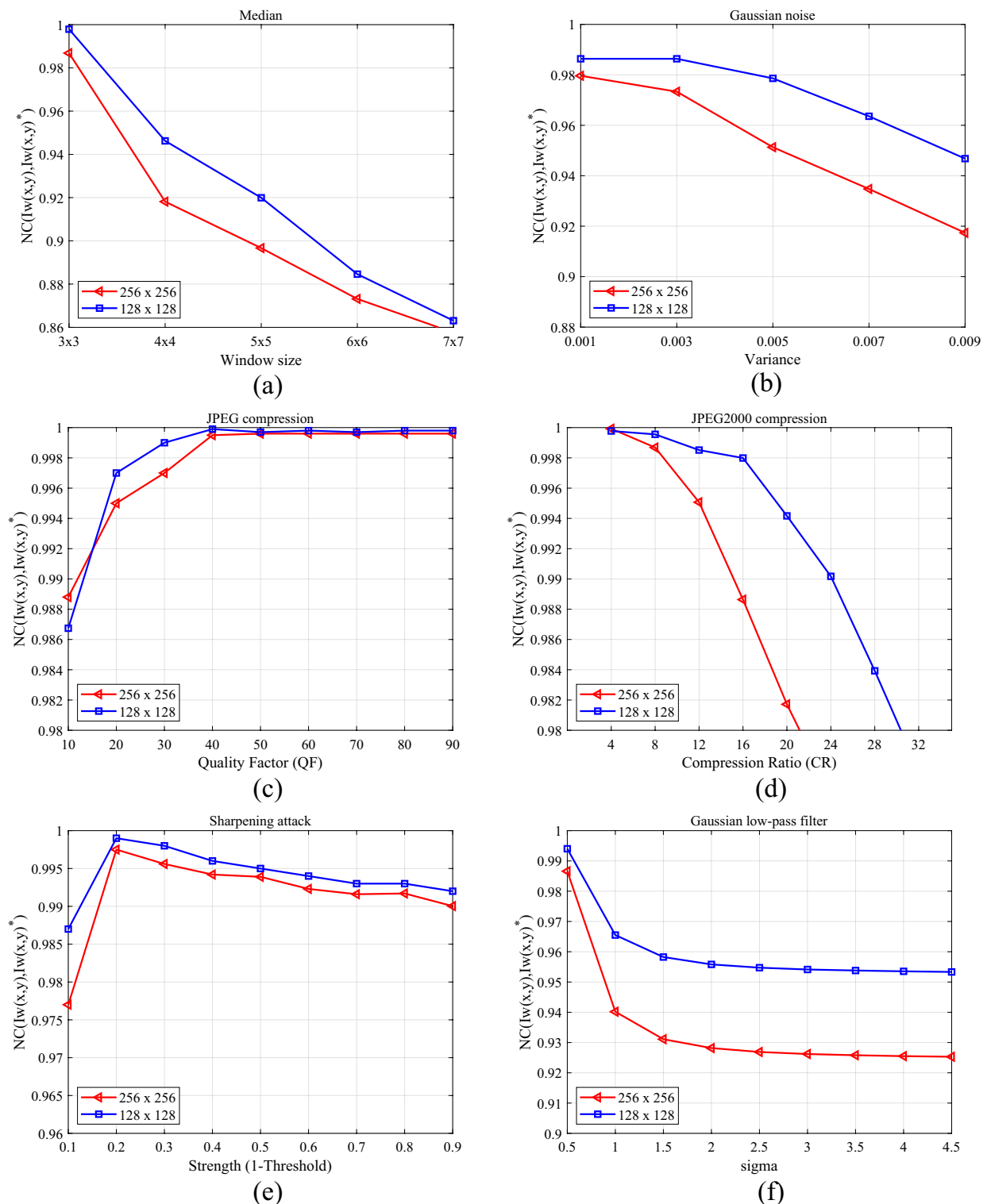


Figure 20. NC value under different parameters under various attacks.

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 9 February 2024; Accepted: 6 August 2024

Published online: 09 August 2024

Methodology	66	67	68	14	17	5	Proposed method
Dimension of water-mark	512 × 512						
Dimension of water-mark	32 × 32	64 × 64	64 × 64	32 × 32	32 × 32	32 × 32	128 × 128
Watermarking Domaine	SVD	SVD	DWT + SVD	RDWT and SVD	Schur	Tucker + SVD	DWT, QR, SVD, QCM
Security	Arnold transform	Arnold transform	Chaotic map	Arnold transform	Affine transform	Arnold transformation	Modified 2D-FrMHHM + key security of QCM
Test dataset	General images	General images	General + Medical + Aerial images	General images	General images	General images	Medical images
Scaling factor	–	–	ABC	ABC	–	–	AOA
NC	0.9984	0.9989	0.9991	0.9994	0.9996	0.9993	0.9998
PSNR	54.876	57.986	59.564	60.564	62.875	64.976	70.342
SSIM	0.9984	0.9989	0.9991	0.9994	0.9996	0.9993	0.9997

Table 9. Comparative analysis of NC, PSNR and SSIM values.

References

- Loan, N. A. *et al.* Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*. **6**, 19876–19897. <https://doi.org/10.1109/ACCESS.2018.2808172> (2018).
- Mali, S. D. & Agilandeswari, L. Non-redundant shift-invariant complex wavelet transform and fractional gorilla troops optimization-based deep convolutional neural network for video watermarking. *J. King Saud. Univ. Comput. Inf. Sci.* **35**(8), 101688. <https://doi.org/10.1016/j.jksuci.2023.101688> (2023).
- Wu, D. *et al.* Robust zero-watermarking scheme using DT CWT and improved differential entropy for color medical images. *J. King Saud. Univ. Comput. Inf. Sci.* <https://doi.org/10.1016/j.jksuci.2023.101708> (2023).
- Fragoso-Navarro, E., Rangel-Espinoza, K., Nakano-Miyatake, M., Cedillo-Hernandez, M. & Perez-Meana, H. Seam Carving based visible watermarking robust to removal attacks. *J. King Saud. Univ. Comput. Inf. Sci.* **34**(7), 4499–4513. <https://doi.org/10.1016/j.jksuci.2021.03.010> (2022).
- Zhang, F. *et al.* A novel robust color image watermarking method using RGB correlations. *Multimed. Tools Appl.* **78**(14), 20133–20155. <https://doi.org/10.1007/s11042-019-7326-9> (2019).
- Bideh, P. N., Mahdavi, M., Borujeni, S. E. & Arasteh, S. Security analysis of a key based color image watermarking vs. a non-key based technique in telemedicine applications. *Multimed. Tools Appl.* **77**(24), 31713–31735. <https://doi.org/10.1007/s11042-018-6218-8> (2018).
- Darwish, S. M. & Al-Khafaji, L. D. S. Dual watermarking for color images: A new image copyright protection model based on the fusion of successive and segmented watermarking. *Multimed. Tools Appl.* **79**(9–10), 6503–6530. <https://doi.org/10.1007/s11042-019-08290-w> (2020).
- Duan, S., Wang, H., Liu, Y., Huang, L. & Zhou, X. A novel comprehensive watermarking scheme for color images. *Secur. Commun. Netw.* <https://doi.org/10.1155/2020/8840779> (2020).
- Begum, M., Ferdush, J. & Uddin, M. S. A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition. *J. King Saud. Univ. Comput. Inf. Sci.* **34**(8), 5856–5867. <https://doi.org/10.1016/j.jksuci.2021.07.012> (2022).
- Prabha, K. & Shatheesh, S. I. An effective robust and imperceptible blind color image watermarking using WHT. *J. King Saud. Univ. Comput. Inf. Sci.* **34**(6), 2982–2992. <https://doi.org/10.1016/j.jksuci.2020.04.003> (2022).
- Zhang, X., Su, Q., Yuan, Z. & Liu, D. An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform. *Optik (Stuttg.)* **219**(July), 165272. <https://doi.org/10.1016/j.ijleo.2020.165272> (2020).
- Li, J., Yu, C., Gupta, B. B. & Ren, X. Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. *Multimed. Tools Appl.* **77**(4), 4545–4561. <https://doi.org/10.1007/s11042-017-4452-0> (2018).
- Abdulrahman, A. K. & Ozturk, S. A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimed. Tools Appl.* **78**(12), 17027–17049. <https://doi.org/10.1007/s11042-018-7085-z> (2019).
- Sharma, S., Sharma, H. & Sharma, J. B. An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. *Appl. Soft Comput. J.* **84**, 105696. <https://doi.org/10.1016/j.asoc.2019.105696> (2019).
- Liu, X. L., Lin, C. C. & Yuan, S. M. Blind dual watermarking for color images' authentication and copyright protection. *IEEE Trans. Circuits Syst. Video Technol.* **28**(5), 1047–1055. <https://doi.org/10.1109/TCSVT.2016.2633878> (2018).
- Zhou, X., Ma, Y., Zhang, Q., Mohammed, M. A. & Damaševičius, R. A reversible watermarking system for medical color images: Balancing capacity, imperceptibility, and robustness. *Electron.* <https://doi.org/10.3390/electronics10091024> (2021).
- Liu, D., Su, Q., Yuan, Z. & Zhang, X. A color watermarking scheme in frequency domain based on quaternary coding. *Vis. Comput.* **37**(8), 2355–2368. <https://doi.org/10.1007/s00371-020-01991-6> (2021).
- Liu, D., Su, Q., Yuan, Z. & Zhang, X. A blind color digital image watermarking method based on image correction and eigenvalue decomposition. *Signal Process. Image Commun.* **95**(April), 116292. <https://doi.org/10.1016/j.image.2021.116292> (2021).
- Su, Q., Niu, Y., Wang, G., Jia, S. & Yue, J. Color image blind watermarking scheme based on QR decomposition. *Signal Process.* **94**(1), 219–235. <https://doi.org/10.1016/j.sigpro.2013.06.025> (2014).
- Nejati, F., Sajedi, H. & Zohourian, A. Fragile watermarking based on QR decomposition and fourier transform. *Wirel. Pers. Commun.* **122**(1), 211–227. <https://doi.org/10.1007/s11277-021-08895-1> (2022).
- Sivananthamaitrey, P. & Kumar, P. R. Optimal dual watermarking of color images with SWT and SVD through genetic algorithm. *Circuits Syst. Signal Process.* **41**(1), 224–248. <https://doi.org/10.1007/s00034-021-01773-y> (2022).
- Yan, M., Jie, J. & Zhang, P. Chaotic systems with variable indexes for image encryption application. *Sci. Rep.* **12**(1), 19585 (2022).
- Kaur, M. & Kumar, V. A comprehensive review on image encryption techniques. *Arch. Comput. Methods Eng.* **27**(1), 15–43. <https://doi.org/10.1007/s11831-018-9298-8> (2020).
- Muñoz-Guillermo, M. Image encryption using q-deformed logistic map. *Inf. Sci. (NY)*. **552**, 352–364. <https://doi.org/10.1016/j.ins.2020.11.045> (2021).
- Qian, X. *et al.* A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. *IEEE Access*. **9**, 61334–61345. <https://doi.org/10.1109/ACCESS.2021.3073514> (2021).

26. Hu, T. Discrete chaos in fractional henon map. *Appl. Math.* **05**(15), 2243–2248. <https://doi.org/10.4236/am.2014.515218> (2014).
27. Tahiri, M. A. *et al.* New color image encryption using hybrid optimization algorithm and Krawtchouk fractional transformations. *Vis. Comput.* **39**(12), 6395–6420. <https://doi.org/10.1007/s00371-022-02736-3> (2023).
28. Bencherqui, A. *et al.* Chaos-enhanced archimede algorithm for global optimization of real-world engineering problems and signal feature extraction. *Processes* **12**(2), 406. <https://doi.org/10.3390/pr12020406> (2024).
29. Bencherqui, A. *et al.* Optimal algorithm for color medical encryption and compression images based on DNA coding and a hyperchaotic system in the moments. *Eng. Sci. Technol. Int. J.* **50**, 101612. <https://doi.org/10.1016/j.jestch.2023.101612> (2024).
30. Hmimid, A. & Sayyouri, M. H. Image classification using novel set of charlier moment invariants. *WSEAS Trans. Signal Process.* **10**(1), 156–167 (2014).
31. Camacho-Bello, C. & Rivera-Lopez, J. S. Some computational aspects of Tchebichef moments for higher orders. *Pattern Recogn. Lett.* **112**, 332–339. <https://doi.org/10.1016/j.patrec.2018.08.020> (2018).
32. Tahiri, M. A. *et al.* Octonion-based transform moments for innovative stereo image classification with deep learning. *Complex Intell. Syst.* <https://doi.org/10.1007/s40747-023-01337-4> (2024).
33. Karmouni, H. *et al.* Secure and optimized satellite image sharing based on chaotic π map and Racah moments. *Expert Syst. Appl.* **236**, 121247. <https://doi.org/10.1016/j.eswa.2023.121247> (2024).
34. Abdul-Hadi, A. M., Abdulhussain, S. H. & Mahmmoud, B. M. On the computational aspects of Charlier polynomials. *Cogent Eng.* <https://doi.org/10.1080/23311916.2020.1763553> (2020).
35. Karmouni, H., Jahid, T., Sayyouri, M., Hmimid, A. & Qjidaa, H. Fast reconstruction of 3D images using Charlier discrete orthogonal moments. *Circuits Syst. Signal Process.* **38**(8), 3715–3742. <https://doi.org/10.1007/s00034-019-01025-0> (2019).
36. Tahiri, M. A., Karmouni, H., Sayyouri, M., Qjidaa, H. *2D and 3D Image Localization, Compression and Reconstruction Using New Hybrid Moments* (Springer US, 2022). <https://doi.org/10.1007/s11045-021-00810-y>.
37. Yamni, M., Karmouni, H., Sayyouri, M., Qjidaa, H. & Flusser, J. Novel Octonion Moments for color stereo image analysis. *Digit. Signal Process. A Rev. J.* **108**, 102878. <https://doi.org/10.1016/j.dsp.2020.102878> (2021).
38. Amakdouf, H., Zouhri, A., Mallahi, E. L. & M, Qjidaa H., Color image analysis of quaternion discrete radial Krawtchouk moments. *Multimed. Tools Appl. Publ. Online* <https://doi.org/10.1007/s11042-020-09120-0> (2020).
39. Dubey, V. Quaternion Fourier transform for colour images. *IJCSIT* **5**(3), 4411–4416 (2014).
40. Sayyouri, M., Hmimid, A. & Qjidaa, H. Image analysis using separable discrete moments of Charlier-Hahn. *Multimed. Tools Appl.* **75**(1), 547–571. <https://doi.org/10.1007/s11042-014-2307-5> (2016).
41. Hmimid, A., Sayyouri, M. & Qjidaa, H. Image classification using separable invariant moments of Charlier-Meixner and support vector machine. *Multimed. Tools Appl.* **77**(18), 23607–23631. <https://doi.org/10.1007/s11042-018-5623-3> (2018).
42. National Library of Medicine—National Institutes of Health. <https://www.nlm.nih.gov/> (accessed 18 Jan 2021).
43. Hassan II University Hospital. http://www.chu-fes.ma/logo_chu-final/.
44. Premkumar, M. *et al.* A new arithmetic optimization algorithm for solving real-world multiobjective CEC-2021 constrained optimization problems: Diversity analysis and validations. *IEEE Access.* **9**, 84263–84295. <https://doi.org/10.1109/ACCESS.2021.3085529> (2021).
45. Abualigah, L., Diabat, A., Mirjalili, S., Abd Elaziz, M. & Gandomi, A. H. The arithmetic optimization algorithm. *Comput. Methods Appl. Mech. Eng.* <https://doi.org/10.1016/j.cma.2020.113609> (2021).
46. Zhou, N. R., Hu, L. L., Huang, Z. W., Wang, M. M. & Luo, G. S. Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. *Expert Syst. Appl.* **238**, 122052. <https://doi.org/10.1016/j.eswa.2023.122052> (2024).
47. Gong, L. H. & Luo, H. X. Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR. *Opt. Laser Technol.* **2023**(167), 109665. <https://doi.org/10.1016/j.optlastec.2023.109665> (2023).
48. Xiaohui, Z. Text information hiding and recovery via wavelet digital watermarking method. *Sci. Rep.* **13**(1), 9532. <https://doi.org/10.1038/s41598-023-36759-0> (2021).
49. Kowalczyk, Y. & Holub, J. Evaluation of digital watermarking on subjective speech quality. *Sci. Rep.* **11**(1), 20185. <https://doi.org/10.1038/s41598-021-99811-x> (2021).
50. Hua, Z., Zhu, Z., Yi, S., Zhang, Z. & Huang, H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf. Sci. (NY)*. **546**, 1063–1083. <https://doi.org/10.1016/j.ins.2020.09.032> (2021).
51. Aminuddin, A. & Ernawan, F. AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. *J. King Saud. Univ. Comput. Inf. Sci.* **34**(8), 5822–5840. <https://doi.org/10.1016/j.jksuci.2022.02.009> (2022).
52. Hu, X., Wei, L., Chen, W., Chen, Q. & Guo, Y. Color image encryption algorithm based on dynamic chaos and matrix convolution. *IEEE Access.* **8**, 12452–12466. <https://doi.org/10.1109/ACCESS.2020.2965740> (2020).
53. Xu, L., Gou, X., Li, Z. & Li, J. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Opt. Lasers Eng.* **2017**(91), 41–52. <https://doi.org/10.1016/j.optlaseng.2016.10.012> (2016).
54. Kumar, V. & Girdhar, A. A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. *Multimed. Tools Appl.* **80**(3), 3749–3773. <https://doi.org/10.1007/s11042-020-09854-x> (2021).
55. Rehman, A. U., Khan, J. S., Ahmad, J. & Hwang, S. O. A new image encryption scheme based on dynamic S-boxes and chaotic maps. *3D Res.* **7**(1), 1–8. <https://doi.org/10.1007/s13319-016-0084-9> (2016).
56. Qayyum, A. *et al.* Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access.* **8**, 140876–140895. <https://doi.org/10.1109/ACCESS.2020.3012912> (2020).
57. Ahmad, J. & Hwang, S. O. Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dyn.* **82**(4), 1839–1850. <https://doi.org/10.1007/s11071-015-2281-0> (2015).
58. Li, Y., Lin, X. & Liu, J. An improved gray wolf optimization algorithm to solve engineering problems. *Sustainability* **13**(6), 3208. <https://doi.org/10.3390/su13063208> (2021).
59. Hou, Y. *et al.* Improved grey wolf optimization algorithm and application. *Sensors* **22**(10), 3810. <https://doi.org/10.3390/s22103810> (2022).
60. Garro, B. A., Rodríguez, K. & Et Vázquez, R. A. Classification of DNA microarrays using artificial neural networks and ABC algorithm. *Appl. Soft Comput.* **38**, 548–560. <https://doi.org/10.1016/j.asoc.2015.10.002> (2016).
61. Liu, J. *et al.* An optimized image watermarking method based on HD and SVD in DWT domain. *IEEE Access.* **7**, 80849–80860. <https://doi.org/10.1109/ACCESS.2019.2915596> (2019).
62. Shen, Y., Tang, C., Xu, M., Chen, M. & Lei, Z. A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO. *Expert Syst. Appl.* **2021**(168), 114414. <https://doi.org/10.1016/j.eswa.2020.114414> (2020).
63. Ansari, I. A., Pant, M. & Ahn, C. W. Robust and false positive free watermarking in IWT domain using SVD and ABC. *Eng. Appl. Artif. Intell.* **49**, 114–125. <https://doi.org/10.1016/j.engappai.2015.12.004> (2016).
64. Singha, A. & Ullah, M. A. Development of an audio watermarking with decentralization of the watermarks. *J. King Saud. Univ. Comput. Inf. Sci.* **34**(6), 3055–3061. <https://doi.org/10.1016/j.jksuci.2020.09.007> (2022).
65. Sun, Y. *et al.* FRRW: A feature extraction-based robust and reversible watermarking scheme utilizing zernike moments and histogram shifting. *J. King Saud. Univ. Comput. Inf. Sci.* **35**(8), 101698. <https://doi.org/10.1016/j.jksuci.2023.101698> (2023).
66. Su, Q., Niu, Y., Zou, H. & Liu, X. A blind dual color images watermarking based on singular value decomposition. *Appl. Math. Comput.* **219**(16), 8455–8466. <https://doi.org/10.1016/j.amc.2013.03.013> (2013).

67. Hu, H. T., Hsu, L. Y. & Chou, H. H. An improved SVD-based blind color image watermarking algorithm with mixed modulation incorporated. *Inf. Sci. (NY)*. **519**, 161–182. <https://doi.org/10.1016/j.ins.2020.01.019> (2020).
68. Sharma, S., Sharma, H., Sharma, J. B. & Poonia, R. C. A secure and robust color image watermarking using nature-inspired intelligence. *Neural Comput. Appl.* <https://doi.org/10.1007/s00521-020-05634-8> (2021).

Acknowledgements

This work was funded by the Researchers Supporting Project Number (RSP2024R102) King Saud University, Riyadh, Saudi Arabia.

Author contributions

M.A.T. and H.K. conceived and designed the study. M.A.T. developed the theory and performed the experiments. M.S., H.Q., M.A. contributed data or analysis tools. M.H., P.P., and O.A., and A.A.A.E. wrote the manuscript, and conducting the security analysis. All authors reviewed the results and approved the final version of the manuscript.

Funding

This project was funded by King Saud University, Riyadh, Saudi Arabia.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.A.A.E.-L.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2024