International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 6, December, 2024, pp. 3327-3334
Journal homepage: http://iieta.org/journals/ts

Optimal Crypto-Watermarking System for Medical Image Protection

Mothi Rajendran[1*], Gokul Chandrasekaran[2], Mahendrakumar Subramaniam[3], Sudha Subramaniam[4]

[1] Department of Biomedical Engineering, Dr. N.G.P. Institute of Technology, Coimbatore 641048, India
[2] Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore 641105, India
[3] Department of Electronics and Communication Engineering, Velalar College of Engineering and Technology, Erode 638012, India
[4] Department of Electronics and Communication Engineering, Kongu Engineering College, Erode 638060, India

Corresponding Author Email: mothi.r@drngpit.ac.in

https://doi.org/10.18280/ts.410648

Received: 15 February 2024
Revised: 3 July 2024
Accepted: 28 August 2024
Available online: 31 December 2024

Keywords:
wavelet packet transform, crypto watermarking, optimal, PSNR

ABSTRACT

Biometrics play a major role in identifying a specific person based on their biological features, and real-time biometric technologies have emerged. Among the other metrics, iris identification is the best and most accurate biometric identification. Intruders can hack the database that stores the collected Iris images, but we can prevent this by enhancing security. We can prevent the use of the wavelet packet transform, particularly at the 3rd level of decomposition, which can break down the cover image into 64 sub bands, by implementing a hybrid watermarking method that combines wavelet packet transformation with a cryptographic technique. Calculating the energy value for each subband yields the watermarked image. We employ AES and grasshopper optimization techniques to bolster the security of the watermarked image. The PSNR value will be used to compare and contrast the watermarked image's quality with the current one.

1. INTRODUCTION

With the advent of new technology, the simplicity and accessibility of accessing digital content have considerably grown. It is also important to note that there have been several instances of illicit reproduction and transmission of digital media. The digital watermark concept emerged as an attempt to solve the problems associated with managing media intellectual property. A digital image watermarking system needs to be resistant to a wide range of potential attacks. Most interesting watermarks are invisible to the naked eye. There are robust and fragile watermarks available for authenticating the images [1]. Standard image processing procedures easily break fragile watermarks, making them effective for tamper detection and authentication. Effective for copyright watermarks, designed to withstand both malicious and unintended attacks, are effective for copyright control techniques is known as steganography [2-4]. Some watermarks conceal data, and these data-obscuring watermarks often exhibit brittleness. watermarks are additional categories of watermarks. When decoding the watermark, a private watermark uses the original image, whereas a public watermark does not use the original image [3, 5, 6].

There are two types of watermarking techniques: those operating in the spatial domain and those in the frequency domain. The impact of spatial domain watermarking and frequency domain watermarking on the item is what distinguishes them. Spatial watermarking is the permanent embedding of an immutable mark, whereas frequency domain watermarking is the application of an orthogonal transformation to the frequency component values. Watermarking based on Discrete Wavelet Transform (DWT) typically embeds spread spectrum watermarks into DWT coefficients. Traditional approaches to watermark detection also use transform techniques to correct the corruption, identify the image's rightful owner, and remove the watermark [7, 8]. The primary goal of watermark detection is to retrieve the watermark. Detection techniques are required to determine the object's location, strength, threshold, or original image. There are times when the incorporation of watermarking technology is required [9, 10].

The development of a secure medical image watermarking method tailored for telemedicine. The approach leverages wavelet transforms to embed watermarks into medical images, ensuring their secure transmission and integrity. This method enhances patient data protection and facilitates secure telemedicine communications, maintaining image quality while providing robust security against unauthorized access and tampering [4, 11, 12].

The paper proposes a robust, invisible watermarking technique specifically designed for biometric image authentication. This technique improves security by embedding an invisible watermark into biometric images, which helps to verify the image's authenticity and integrity. The proposed method is highly secure and aims to protect digital images against unauthorized access and tampering, ensuring that biometric data remains reliable and authentic during transmission and storage [3, 13, 14].

The rest of this article is organized as follows: In Section 2, the Wavelet Packet Transform is described. In Section 3, the Grasshopper Optimization Algorithm is described. In Section 4, Opposition-Based Learning is described in detail. The Optimal Advanced Encryption Standard is described in Section 5. In Section 6, the optimal crypto-watermarking system, Biometric Protection, is described. In Section 7, Results and Discussion are presented. The conclusion of the work is presented in Section 8.

2. WAVELET PACKET TRANSFORM

Wavelet packet transformations can be thought of as a class of transforms with a broader scope than other sorts of transforms. Only the low-pass filter iterates in the wavelet transform. People believe that lower frequencies convey more significant information than higher frequencies [5, 15]. Several signals contradict this premise. The tree's nodes correspond to specific wavelet packet bases. Wavelet packets make use of a basic 2-channel filter bank that can switch between high-pass and low-pass branches. There is a significant difference between the wavelet packet transform and the wavelet transform. To construct wavelet packets, the frequency axis is divided into intervals of varying lengths. As a result, the bases are particularly well suited to deconstructing images with a variety of behaviors at different frequency intervals [16-18].

3. GRASSHOPPER OPTIMIZATION ALGORITHM

People commonly regard certain insects, like grasshoppers, as pests. Usually, people recognize these animals as parasites due to the serious harm they inflict on crops, which affects agricultural productivity. Generally, grasshoppers live alone in nature, but they often join large swarms among all creatures in the environment. Grasshoppers move in large swarms, and the sheer size of these swarms can be a formidable challenge for farmers. Regardless of their development, grasshoppers exhibit the characteristic swarming behavior. Millions of nymph grasshoppers move in a cylindrical pattern. As they're moving, they eat whatever plant gets in their way. Having metamorphosed into adults from nymphs, grasshoppers form large swarms, and they travel over long distances.

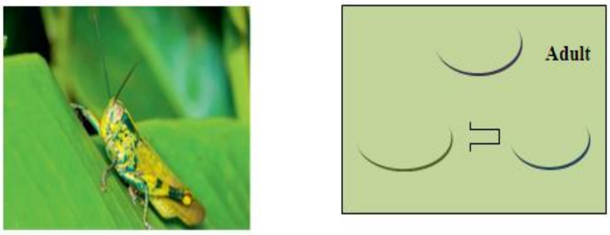


Figure 1. Basic diagrammatic representation of grasshopper

Figure 1 shows the basic diagrammatic representation of a grasshopper. At the larval stage, the swarm movement is exceptionally moderate. The grasshopper's slight bounce plays a crucial role in the swarm's movement during the larval stage. During every stage of differentiation, from larval to adulthood, the swarm's element undergoes a long separation, characterized by unexpected development. It is quite normal for grasshoppers to swarm in search of food [4]. Exploration and exploitation are the two propensities of nature-driven calculation. The two propensities are observed in grasshoppers normally, in which they move unexpectedly just as locally in little zones looking for food. Optimization calculation is a nature-inspired numerical model displayed on the behavior of grasshoppers.

Eq. (1) is used to provide a mathematical representation of the collective behavior of grasshoppers.

$$P_j = S_j + G_j + W_j \tag{1}$$

The variables in the equation under consideration are P_j, S_j, G_j, and W_j. These variables represent the grasshopper's location, interactions with other insects, the effect of gravity, and the result of wind advection, in that order. If the grasshopper has the random behavior, the Eq. (1) can be written as Eq. (2).

$$P_j = R_1 S_j + R_2 G_j + R_3 W_j \tag{2}$$

Random numbers R_1, R_2 and R_3 are in [0,1].

$$S_j = \sum_{k=1, k\neq j}^{O} (e_{jk})\, \vec{e}_{jk} \tag{3}$$

where, e_{jk} is the distance between the j^th^ and the k^th^ grasshopper, calculated as:

$$e_{jk} = |p_k - p_j| \tag{4}$$

The unit vector e_{jk} represents the link between grasshoppers j and k. This demonstrates how the e_{jk} exponential function can be used to indicate the amount of the social force, given as t.

$$\vec{e}_{jk} = \frac{p_k - p_j}{e_{jk}} \tag{5}$$

The t function, represents the social forces as follows:

$$t(s) = gf^{\frac{-s}{m}} - f^{-s} \tag{6}$$

where, g refers to attraction intensity and m is the attractive length scale.

The "t" function depicts the impact of attraction and repulsion on grasshopper social connections.

The gravity force (G_j) is considered in Eq. (7).

$$G_j = -g\hat{e}_g \tag{7}$$

where, g represents the gravitational constant, $\hat{e}_g$ represents a unity vector towards the earth center. The wind advection W_j is measured in Eq. (8).

$$W_j = u\hat{e}_w \tag{8}$$

where, u represents the drift and $\hat{e}_w$ represents a unit vector in the wind direction. The substituting values G, S, and W in Eq. (8).

$$P_j = \sum_{\substack{k=1 \\ k\neq 1}}^{N} S(|P_k - P_k|)\frac{P_k - P_j}{d_{kj}} - g\hat{e}_g + u\hat{e}_w \tag{9}$$

N represents the Number of grasshoppers and $s(r) = fe^{\frac{-r}{l}} - e^{-r}$. The solution is updated in Eq. (9).

4. OPPOSITIONAL BASED LEARNING (OBL)

Opposition-Based Learning (OBL) is an efficient technique for the differential equation evolution problem in optimization. The solution X is evaluated for a problem, and the X opposition solution is generated to find a better solution X'. By continuously performing the above process, we can minimize the distance between the optimal solution and X [1, 7]. For instance, when the value of X is -20 and the optimal solution is 40, we calculate the X' value to be 20 and the X distance to be 60. However, we measure the actual distance of X' as the optimal solution to be 40. Consequently, we calculate the X' to be closer to the optimum solution, which is 40.

$$X' = a + b - X \tag{10}$$

If the answer involves a vector with several dimensions, a similar expansion of the opposition-based learning process can be used. Assume $P(X_1, X_2, \ldots., X_n)$ represents the n-dimensional space width solution and $X_i \in [a_i, b_i] \forall i \in \{1,2,\ldots n\}$. The opposite solution $OP(X_1', X_2', \ldots., X_n')$ is defined below:

$$X_i' = a_i + b_i - X_i \tag{11}$$

5. OPTIMAL ADVANCE ENCRYPTION STANDARD (OAES)

AES is a 128-bit block cipher method. Cryptographic keys of different lengths 128 bits, 192 bits, 256 bits, to be exact help the system function. In this chapter, AES with 128-bit key length is utilized. AES algorithm is used to encrypt the biometric information and project the original information from malicious. Basically, the AES algorithm consists of ten rounds. In this both rounds are having similar calculation except from the last round [19, 20].

Here 10 rounds are used to generate the key of size 128 bits using AES algorithm.

AES is a 128-bit block cypher method. Cryptographic keys of different lengths-128 bits, 192 bits, 256 bits, to be exact-help the system function. This chapter utilizes AES with a 128-bit key length. The AES algorithm is used to encrypt the biometric information and protect the original information from malicious. Basically, the AES algorithm consists of ten rounds. In this case, both rounds have similar calculations, except for the last round [21, 22].

Here, the AES algorithm generates the key of size 128 bits over 10 rounds.

Step 1: Solution initialization

At first, the key values of AES algorithm are randomly selected. In this, the n number of solution is initially crested. The solution is given in Eq. (12):

$$S_i = \{s_1, s_2, \ldots.. s_n\} \tag{12}$$

where, n matches to the individual numbers and S_i denotes the ith individual solution, where the key value represents each solution.

Step 2: Opposite solution generation

When machine learning is used with the One-Bit Learning (OBL) framework, the resulting response contradicts the initial one. S_i has a unique opposite solution of S_i'. $OP(S'_1, S'_2, \ldots, S'_n)$ is measured in the equation:

$$S_i' = L_i + U_i - S_i \tag{13}$$

where, L_i represents the lower bound coefficient, U_i represents the upper bound coefficient, S_i represents the old solution.

Step 3: Fitness calculation

After solution generation, fitness is calculated. Based on the fitness value the best key value is selected. The fitness function is given in Eq. (14).

$$Fitness = keybreakingtime \tag{14}$$

Step 4: Updation using GOA

Using Eq. (15), it is possible to adjust the output once the fitness value has been determined.

$$P_i = S_j + G_i + W_j \tag{15}$$

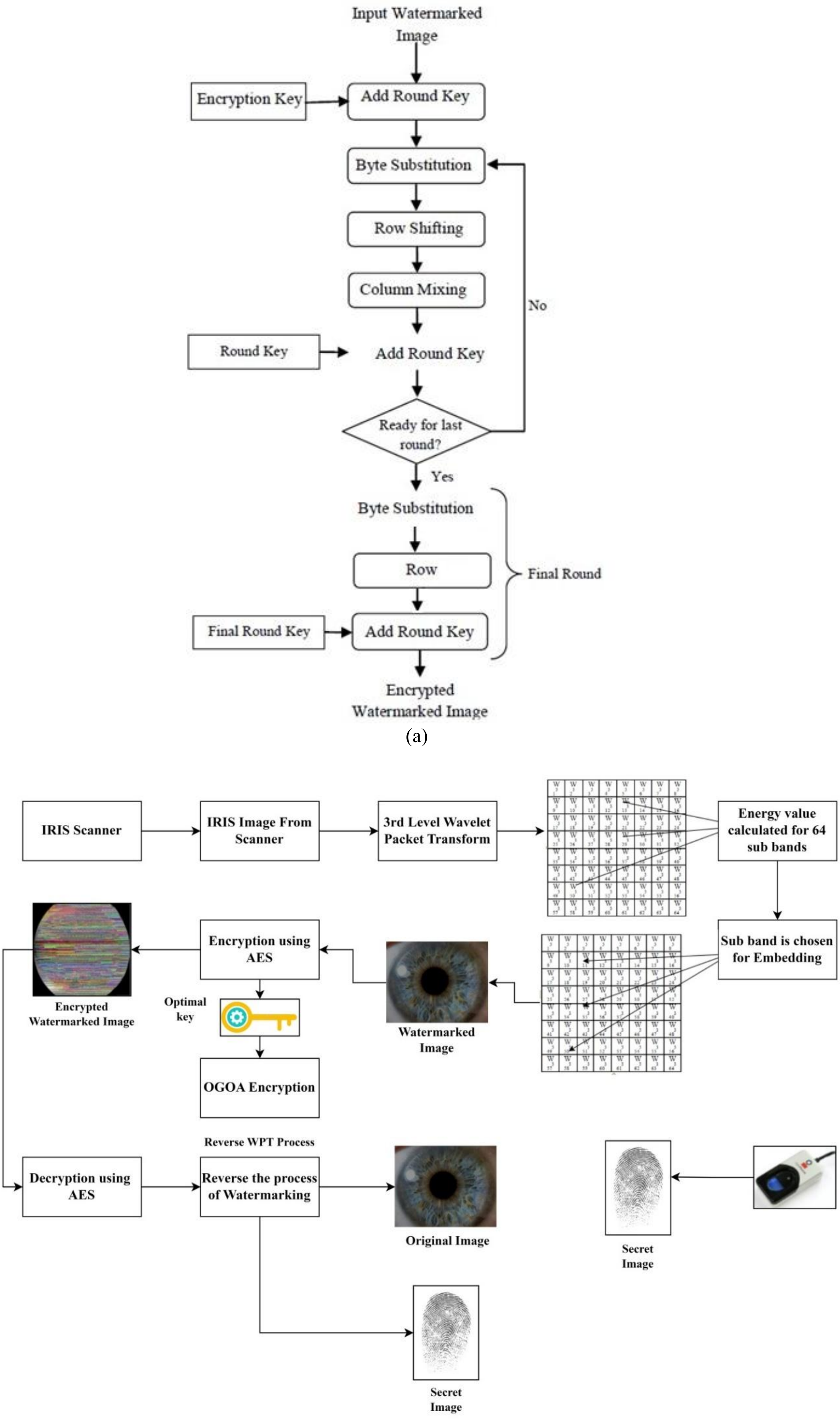
Step 5: Termination criteria

The algorithm works on maximum iteration met. In this work, 50 iteration is utilized. In this value of the best fitness is chosen. The selected fitness value (key) is given to the AES algorithm.

6. OPTIMAL CRYPTO-WATERMARKING SYSTEM BASED BIOMETRIC PROTECTION

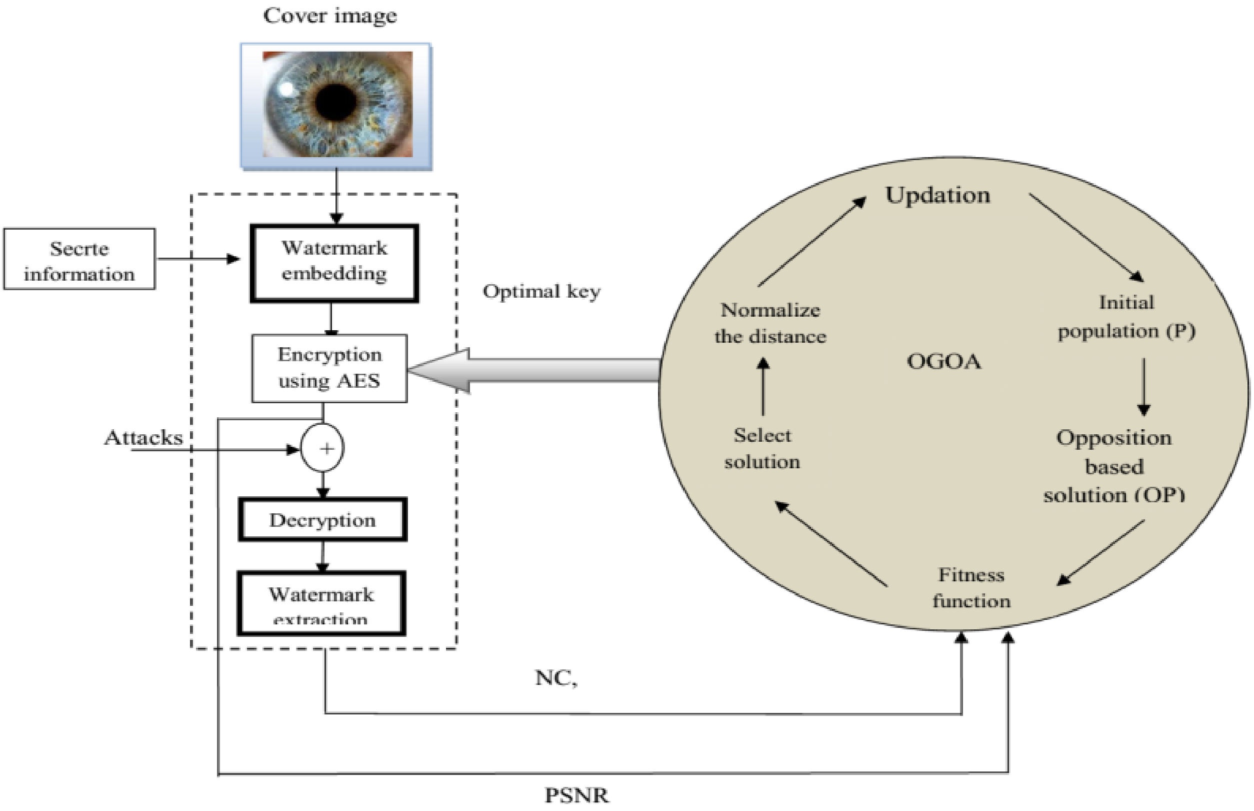
The IRIS scanner is used to scan the human eye and the output of the scanner is represented as IRIS image which is used as original / cover image and it is given as input to the proposed watermarking system. The original image is further decomposed by applying Wavelet transform, especially 3rd level wavelet packet transform is applied for decomposition. The decomposed cover image consists of 64 sub bands on decomposed the image using 3rd level wavelet packet transforms. The energy values are calculated for all the 64 sub bands of decomposed image and the band with minimum energy values are chosen for hiding the secret/watermark image and to get the watermarked image it takes inverse wavelet packet transform. The secret / watermark image is obtained from the finger print recognition device used as shown in Figure 2 (a). Here the AES encryption algorithm is used for securing the watermarked image with more security by 128 bits is used for generation of AES key therefore it requires 16 bytes to perform. The optimal key is selected using the grass hopper optimization technique along with AES. Then the encrypted watermarked image is obtained as shown in the block diagram. In the receiver side the decryption of the watermarked image is obtained by AES algorithm and the reverse process of watermarking technique is carried out. Hence the cover image and the secret/watermark image are reconstructed.

An optimal crypto-watermarking system protects the biometric information. Crypto-watermarking technology is capable of both watermarking and encryption. To increase system security, the key values of AES are optimally selected [8, 13].


Input Watermarked Image
Encryption Key
Add Round Key
Byte Substitution
Row Shifting
Column Mixing
No
Round Key
Add Round Key
Ready for last round?
Yes
Byte Substitution
Row
Final Round
Final Round Key
Add Round Key
Encrypted Watermarked Image
IRIS Scanner
IRIS Image From Scanner
3rd Level Wavelet Packet Transform
Energy value calculated for 64 sub bands
Sub band is chosen for Embedding
Encryption using AES
Encrypted Watermarked Image
Optimal key
OGOA Encryption
Watermarked Image
Reverse WPT Process
Decryption using AES
Reverse the process of Watermarking
Original Image
Secret Image
Secret Image

(a)

(b)



(c)

Figure 2. (a) Flow diagram of AES algorithm; (b) Block diagram of proposed methodology; (c) Block diagram of OGOA algorithm

In that sequence, the suggested methodology consists of four stages: extraction, key optimisation, encryption, and watermark integration. The proposed methodology overall diagram is shown in Figure 2 (b).

Step 1: Image transformation using wavelet packet decomposition (WPD)

Consider the cover image I^{in}. In this chapter, at first, 3LWPD is applied to cover image to decompose the image. 3LWPD sixty-four subbands are obtained.

Step 2: Suitable subband selection

After decomposition, the band with minimum energy is selected for further processing. Energy is calculated using Eq. (16)

$$E = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(x(i,j)\right)^2 \tag{16}$$

where, *n* and *m* denote the column and row value of sub band.

Step 3: Embedding process

After, suitable band selection, the watermark bit W^{in} is embedded into the selected band. The watermark bit W^{in} is derived from the secrete image I^{s}. The embedding of watermark with the original image is processed as given in Figure 2. After attaining watermarked image, the inverse IWPD is applied to get the watermarked image I^{water}.

Step 4: OAES based encryption

After the embedding process, to increase the security of the image, the OAES based encryption is applied to the watermarked image I^{water} which will give the extra security. In encryption process, the watermarked image I^{water} is encrypted and obtain an encrypted image I^{En}. The watermarked and encrypted image was either sent across a network or securely stored in a database for subsequent access.

Step 5: Extraction process

After the embedding process, the extraction process is carried out. The reverse process of embedding is done in the extraction process. Here, at first, encrypted image I^{En} is decrypted using a decryption algorithm and obtained I^{de}. Then in this I^{de} image, the watermark extraction process is applied. Finally, the original image I^{in} and secret information I^{s} are obtained.

7. RESULTS AND DISCUSSION

This section develops the optimal crypto-watermarking system for image protection. We have implemented the proposed work in MATLAB. Here, for experimental analysis, ten images are used. Figure 3 represents the test images for analysis.

CASIA dataset and UBIRIS dataset images are used for biometric secure sharing. One of the databases used in the experimentation is the Chinese Academy of Sciences Institute of Automation (CASIA). It contains 756 grayscale eye images, each containing 108 unique eyes or classes and 7 dissimilar images. Each database iris image has a size of 280×320 pixels. As a result, there are a total of 756 (108×7) images in the database.

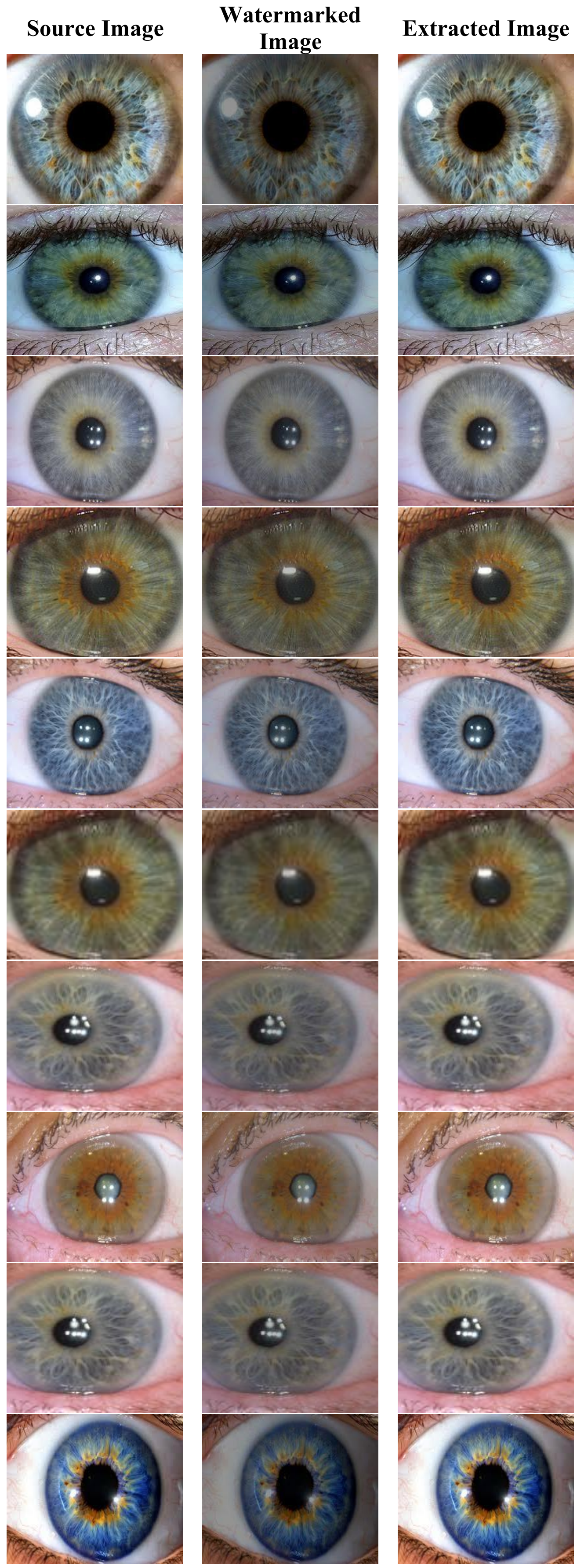


Figure 3. Test images for analysis

Table 1 illustrates the performance of the proposed approach using PSNR values in dB and embedding capacity. This paper uses a total of ten images for experimental analysis.

Table 2 represents the proposed approach's performance analysis using the NC measure. The proposed approach has an average NC of 0.995, which is its maximum value. Figure 4 displays the graphical picture of the NC measure. When analyzing Table 3, the proposed method reaches the maximum PSNR of 59.567, 58.3261, 58.9483, 60.15, 57.374, 50.3845, 52.578, 54.468, 60.04, and 53.1942 for images 1 to 10, respectively. The embedded capacity is 1024 bits. Figure 5 displays a graphical representation of the PSNR measure.

Table 3 shows the performance analysis for the proposed approach using the MSE measure. The minimum error value gives a better result. We use ten images for the experimental analysis. When analyzing Tables 3 and 4, the proposed approach attains a minimum error value of 0.2563, 0.3124, 0.572, 0.1432, 0.16, 0.647, 0.573, 0.474, 0.743, and 0.645 for images 1 and 10, respectively. Figure 6 provides a graphical representation of the MSE measure output for ten images.

Table 1. Proposed approach using embedding capacity (bits) and PSNR value (dB)

Proposed Optimal Crypto Watermarking System			
Images	File Format	PSNR in db	Embedding Capacity in bits
Image-1	JPEG	59.56	1024
Image-2		58.32	
Image-3		58.94	
Image-4		60.15	
Image-5		57.37	
Image-6		50.38	
Image-7		52.57	
Image-8		54.46	
Image-9		60.04	
Image-10		53.19	
Average		**56.503**	

Table 2. Proposed approach using NC and embedding capacity (bits)

Proposed Optimal Crypto Watermarking System			
Images	File Format	NC	Embedding capacity in bits
Image-1	JPEG	1	1024
Image-2		1	
Image-3		0.9986	
Image-4		1	
Image-5		1	
Image-6		0.9943	
Image-7		0.9841	
Image-8		0.9923	
Image-9		0.9945	
Image-10		0.9862	
Average		**0.995**	

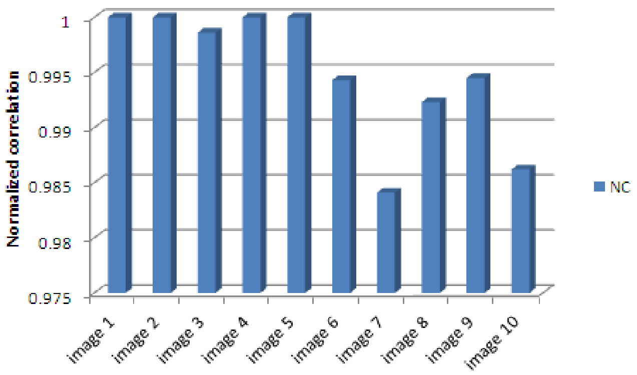


Figure 4. Performance analysis based on NC measure

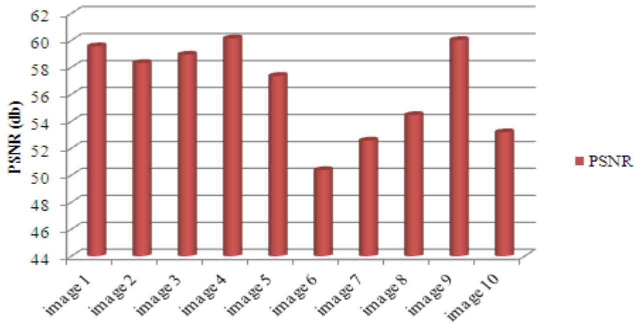


Figure 5. Performance analysis based on PSNR measure

Table 3. Performance of proposed method using MSE

Proposed Optimal Crypto Watermarking System			
Images	File Format	MSE	Embedding capacity (bits)
Image-1	JPEG	0.2563	1024
Image-2		0.3124	
Image-3		0.572	
Image-4		0.1432	
Image-5		0.16	
Image-6		0.647	
Image-7		0.573	
Image-8		0.474	
Image-9		0.743	
Image-10		0.645	
Average		**0.4525**	

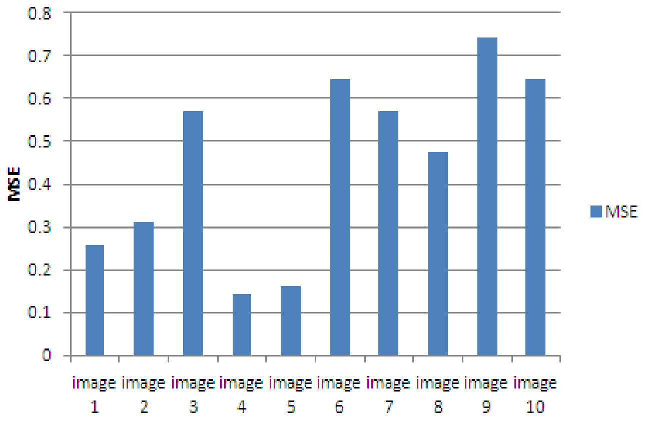


Figure 6. Performance analysis based on MSE measure

A comparison analysis with different algorithms determined the proposed method's performance to be favourable. Here, the proposed optimal crypto watermarking system is compared with a three-level discrete wavelet transform-based watermarking system (3LDWT) and a crypto-watermarking system.

Table 4 shows the comparative analysis based on the PSNR measure. When analyzing Table 1, the proposed algorithm attains a maximum PSNR of 59.567, 58.3261, 58.9483, 60.15, 57.374, 50.3845, 52.578, 54.468, 60.04, and 53.1942 for images 1 and 10, respectively. Similarly, the 3LDWT-based watermarking system attains a PSNR of 49.567, 48.326, 48.948, 48.997, 47.374, 46.385, 45.578, 44.468, 48.368, and 42.194 for images 1 to 10, respectively. Similarly, the system achieves a PSNR of 55.647, 53.573, 54.743, 55.437, 52.468, 51.37, 48.463, 48.3472, 53.426, and 46.427 for images 1 to 10, respectively. It is evident from the table that the proposed algorithm achieves the highest PSNR in comparison to the alternative methods.

Table 4. Comparative analysis based on PSNR measure

Images	**3LDWT Based Watermarking**	**Crypto-Watermarking System**	**Proposed Method**
Image-1	49.567	55.647	59.567
Image-2	48.326	53.573	58.326
Image-3	48.948	54.743	58.948
Image-4	48.997	55.437	60.15
Image-5	47.374	52.468	57.374
Image-6	46.385	51.37	53.385
Image-7	45.578	48.463	52.578
Image-8	44.468	48.3472	54.468
Image-9	48.368	53.426	60.04
Image-10	42.194	46.427	53.194

Table 5. Performance analysis based on different optimization algorithm

Images	**GOA**	**GA**	**FA**	**OGOA (Proposed)**
	+ Crypto Watermarking			
Image-1	55.374	53.574	52.352	59.567
Image-2	54.243	51.472	50.647	58.326
Image-3	53.647	49.472	48.536	58.948
Image-4	55.342	52.432	51.243	60.15
Image-5	52.376	50.643	49.412	57.374
Image-6	50.573	48.464	47.427	53.385
Image-7	49.474	47.479	46.853	52.578
Image-8	50.463	49.437	48.721	54.468
Image-9	55.357	53.462	52.741	60.04
Image-10	50.352	48.462	47.215	53.194

Table 5 shows the performance analysis based on different optimization algorithms. For comparison, the grasshopper optimization algorithm (GOA), the genetic algorithm (GA), and the firefly algorithm (FA) are utilized. Upon analyzing Table 1, we find that the proposed approach achieves a peak PSNR value of 60.15db. This value is 55.374db when using GOA with crypto-watermarking, 53.574db when using GA with crypto-watermarking and 52.741db when using FA with crypto-watermarking. Table 1 clearly demonstrates that the proposed OGOA+ crypto watermarking system achieves superior results when compared to other methods.

8. CONCLUSION

While recent technological advancements offer numerous benefits to society, they also raise numerous concerns, particularly regarding the privacy of user data exposed to an open network. As a result, numerous researchers have developed a variety of security-based systems. They are highly focused on safeguarding the confidentiality of users' data. Cryptography-based techniques and watermarking are some of the most effective data security techniques. However, traditional cryptographic techniques prove ineffective on multimedia platforms, leading to the emergence and successful application of the crypto-watermarking technique in various fields. The objective of this proposed work is to transmit medical-related information from one place to another without losing any data using different encryption and watermarking algorithms. As previously discussed, there are numerous approaches to secure transmission. This approach divides the proposed concept into three parts. The first part develops discrete wavelet transform (DWT)-based watermarking for secure transmission. The second part develops a crypto-watermarking system to improve PSNR and image quality. Here, the watermarking process employs a wavelet packet transform and the encryption AES algorithm. The crypto-watermarking system produced high PSNR and NC compared to DWT-based watermarking. In the third section, we develop an optimal crypto-watermarking system for the secure transmission of medical images. The method yields a higher level of security compared to alternative methods. The experimental results of both phases are examined using PSNR measures and visual quality on the MATLAB platform. The quality of the watermarked image has been observed and compared with other existing techniques, achieving an average PSNR of 56.503dB. The increase in PSNR compared to grasshopper optimization is 4%, and the genetic algorithm is 6%, which effectively increases the image's quality.

REFERENCES

[1] Borra, S., Thanki, R. (2020). Crypto-watermarking scheme for tamper detection of medical images. Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 8(4): 345-355. https://doi.org/10.1080/21681163.2019.1595730

[2] Aparna, P., Kishore, P.V.V. (2018). An efficient medical image watermarking technique in E-healthcare application using hybridization of compression and cryptography algorithm. Journal of Intelligent Systems, 27(1): 115-133. https://doi.org/10.1515/jisys-2017-0266

[3] Garg, P., Jain, A. (2023). A robust technique for biometric image authentication using invisible watermarking. Multimedia Tools and Applications, 82(2): 2237-2253. https://doi.org/10.1007/s11042-022-13314-z

[4] Moad, M.S., Kafi, M.R., Khaldi, A. (2022). A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocessors and Microsystems, 90: 104490. https://doi.org/10.1016/j.micpro.2022.104490

[5] Priya, S., Santhi, B. (2021). A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. Mobile Networks and Applications, 26(6): 2501-2508. https://doi.org/10.1007/s11036-019-01213-x

[6] Sushma, C.H., Kumari, P.L.S. (2021). Analysis on visual cryptography to secure image by using digital watermarking. Solid State Technology, 64(2): 203-208.

[7] Mothi, R., Karthikeyan, M. (2019). Protection of bio medical iris image using watermarking and cryptography with WPT. Measurement, 136: 67-73. https://doi.org/10.1016/j.measurement.2018.12.030

[8] AthishMon, F., Suthendran, K. (2018). Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems. International Journal of Pure and Applied Mathematics, 118(8): 265-269.

[9] Alhussan, A.A., Abdallah, H.A., Alsodairi, S., Ateya, A.A. (2023). Hybrid watermarking and encryption techniques for securing medical images. Journal of Computer Science & Engineering, 46(1): 403-416. http://dx.doi.org/10.32604/csse.2023.035048

[10] Kumar, J., Singh, A.K. (2023). Copyright protection of medical images: A view of the state-of-the-art research and current developments. Multimedia Tools and Applications, 82(28): 44591-44621. https://doi.org/10.1007/s11042-023-15315-y

[11] Gull, S., Parah, S.A. (2024). Advances in medical image watermarking: A state of the art review. Multimedia Tools and Applications, 83(1): 1407-1447. https://doi.org/10.1007/s11042-023-15396-9

[12] Moad, M.S., Kafi, M.R., Khaldi, A. (2022). Medical image watermarking for secure e-healthcare applications. Multimedia Tools and Applications, 81(30): 44087-44107. https://doi.org/10.1007/s11042-022-12004-0

[13] Juvvanapudi, S.R.V., Kumar, P.R., Reddy, K.V.V. (2021). An optimal and hybrid encryption-based integer wavelet transform with DCT for color image watermarking. Turkish Online Journal of Qualitative Inquiry, 12(5): 5029-5049.

[14] Ray, A., Roy, S. (2020). Recent trends in image watermarking techniques for copyright protection: A survey. International Journal of Multimedia Information Retrieval, 9(4): 249-270. https://doi.org/10.1007/s13735-020-00197-9

[15] Gaurav, K., Ghanekar, U. (2018). Image steganography based on Canny edge detection, dilation operator and hybrid coding. Journal of Information Security and Applications, 41: 41-51. https://doi.org/10.1016/j.jisa.2018.05.001

[16] Gajul, S., Gite, A., Kedari, V., Kumbhar, P. (2016). Secure data sharing using visual cryptography and watermarking method in fog computing. International Research Journal of Engineering and Technology, 3(10).

[17] Rashid, A. (2016). Digital watermarking applications and techniques: A brief review. International Journal of Computer Applications Technology and Research, 5(3): 147-150.

[18] El Bireki, M.F.M., Abdullah, M.F.L., Ukasha, A.A.M., Elrowayati, A.A. (2016). Digital image watermarking based on joint (DCT-DWT) and Arnold Transform. International Journal of Security and Its Applications, 10(5): 107-118. http://doi.org/10.14257/ijsia.2016.10.5.10

[19] Mothi, R., Karthikeyan, M. (2014). Color image watermarking using wavelet packet transform. In 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, pp. 1-5. https://doi.org/10.1109/ICCIC.2014.7238562

[20] Mothi, R., Karthikeyan, M. (2013). A wavelet packet and fuzzy based digital image watermarking. In 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, India, pp. 1-5. https://doi.org/10.1109/ICCIC.2013.6724292

[21] Jawad, K., Khan, A. (2013). Genetic algorithm and difference expansion based reversible watermarking for relational databases. Journal of Systems and Software, 86(11): 2742-2753. https://doi.org/10.1016/j.jss.2013.06.023

[22] Kumar, Y., Munjal, R., Sharma, H. (2011). Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies, 11(3): 60-63.