International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure Image Encryption Model with Compressive Sensing and Addition of Watermarking Approach

Shaik Kashif Hussain[1]*, S. Saheb Basha[2]

Submitted:01/01/2024 **Revised:**02/02/2024 **Accepted:**11/02/2024

Abstract: In modern times, protecting medical images is essential to maintaining the accuracy of patient confidential data. One effective method for content-based authentication is watermarking. Multimedia files are first watermarked and then deleted for authentication reasons, according to the conventional watermarking procedure. Conventional watermarking models perform poorly due to their resilience and recovery capabilities, and there is currently no digital watermarking solution that provides total security from any type of attack. To solve these problems, including tamper localization and recovery, novel image authentication based on compressive sensing and watermarking is used. The novel image encryption technique presented in this paper is based on the idea of tamper localization. By detecting and eliminating illegal image modifications, tampering localization is essential for improving image quality. This article presents an ADTCWT, an adaptive dual-tree complex wavelet transform, which splits the input picture into high-frequency and low-frequency versions. In this scenario, the ISEO fine-tunes the ADTCWT's parameters. The processed low- and high-frequency pictures are encrypted using the adaptive 2D logistic chaotic encryption (A-2DLCE) model. The improved ISEO is used to choose the keys for encryption. After that, you may get the original images back by doing an inverse decomposition with the inverse ADTCWT. Also, A-2DLCE gets the encrypted data so that it can decode the images. The reconstructed watermark has very little visible deformation, which keeps it authentic. The experiment showed that the proposed method is less visible and more durable than the present watermarking methods.

Keywords: *Compressive sensing, Image Encryption, Tamper localization, Transforms, SSIM, MSE Switched capacitor circuits, Integrated circuits.*

1. Introduction

Every day, the Internet converts and transports a vast amount of electronic data. As digital processes and data storage continue to advance at a rapid pace, more and more digital data is being transformed and sent via the internet every day. People are at danger of security problems when they do things like this [2]. As more and more people use web-based apps, the chances of assaults on digital photographs sent over public networks go up [3]. People who don't pay attention often get images that have viruses in them. The data is greatly affected by these pictures [4]. The military, the government, and forensics are some of the fields that have been struck heavily. So, keeping personal information safe is very important to keep it hidden. People are starting to realize how important it is to protect their private information when they send it online. In previous studies, methods such as image information concealment, graphic identification, and image encryption were used to achieve electronic image safety [5]. There are two main types of image authentication methods: quality verification and material verification. Quality verification uses several encryption techniques to prevent images from having little influence on image attributes [6]. A secure encryption method can shield sensitive information from prying eyes and even thwart hackers. Strong image encryption methods are required since the Internet platform transmits millions of data records every day. Data security is ensured by encryption techniques, which allow for a well-protected transfer of data. Therefore, traditional methods heavily rely

[1] *Research Scholar, JNT University, Ananthapuramu and Assistant Professor of ECE Department, Rajeev Gandhi Memorial College of Engineering And Technology (Autonomous), Nandyal, Andhra Pradesh, India*
[2] *Professor, Department of ECE, G.Pulla Reddy Engineering College (Autonomous), Kurnool, Andhra Pradesh, India.*
** Corresponding author's Email: kashif1919@gmail.com*

on tamper localization and tamper identification to improve picture quality [7]. The paradigm for authenticating images comprises two main components: content authentication and integrity authentication. In integrity authentication, even minor edits to the image are prohibited. Digital watermarks and signatures can show that images are authentic [8]. The watermark commonly uses digest settings to get back images that have been changed. It's not too hard to correct things when the low-frequency bits or watermark bits are broken. It can suggest that the system's accuracy is going decreased if enhanced recovery isn't operating as well [9]. The image encryption works can separate pixels in an image, which makes them less connected to each other. The encrypted picture poses a huge danger to the security of the original material since an attacker could find out the encryption key and get to the information. It's hard to see the hidden data, thus methods for hiding information focus on adding authentication or crucial data to the original picture [10–11].

It is essential for image authentication to establish if the quality of an image has been modified due to technological advancements so that recipients may confirm the validity and integrity of the information they have received. Conventional authentication techniques are based on integrity authentication, which is useless for checking the legitimacy of an image, as it prohibits any modification of the sent data. But most recent methods of digital signatures and watermarking can only check that the contents of photos are real or that they are whole. These hidden visuals are used by the military and the medical industry to protect private messages. The individual who concealed the data can get it post-encryption of the picture. Utilizing confidential information from the recipient's side significantly simplifies the process of identifying missing data, determining its location, and verifying alterations. This ensures the data arrives securely and is not lost [12–13].

Various methods for encrypting images have been covered in academic works; some of them include symmetric and asymmetric encryption, chaotic maps, and encrypted images. The encryption approach allows for enhanced privacy protection. A vital component of most encryption techniques, the encryption key ensures the data's encrypted integrity and keeps sensitive information safe. If someone breaks into your computer and steals the encrypted picture, they might put the real data at risk by trying to figure out the encryption or by stealing the encryption key [14–15]. The purpose of encryption is to make the grayscale smoother and break the links between the image's pixels. Adding an image to a document makes it more complicated by causing the pixel positions to become jumbled, making it challenging for the human eye to differentiate between them. We can conceal the intensity of the photograph's edge details using a similar technique. "External file inserting" is a means to hide secret data and keys in a picture of cover art. When individuals wish to find a photo, they often check at the digital watermarks and digital signatures first. The watermark's main job is to help get back data that has been changed, even though digested readings are the best approach to discover changes [23-25].

Conventional image encryption methods achieve insufficient security and efficacy by use of many cycles of dispersion and disorientation. CS-based tamper localization aids in identifying anonymous characteristics for identifying and localizing unauthorized modifications. Because of its ability to detect tampering in real-time, it is perfect for scenarios requiring an immediate response [16]. There is no new way that can solve the problems with current encryption image approaches, such as their ineffectiveness and lack of cryptographic capability. The huge quantity of data needed to be concealed makes traditional methods of data concealment ineffective. Also, it affects personal data security in other ways. There are a lot of challenges with the traditional system, such as difficulties with online storage and transfer and the difficulty of maintaining secrecy and safety. During distribution, the conventional technique uses up a large chunk of the image's storage space. People are worried about how long it will take, and it doesn't address the privacy and security problems with health pictures taken from trustworthy sources. It's not only risky, but it's also unreliable, doesn't follow the rules, and is hard to use. Old algorithms have also used low-resolution photos to their advantage [17] [26-30].

As a result, we focused on a robust image encryption solution to address the current problems, and its contents are detailed below.

- ➢ The development of an effective image encryption model utilizing a heuristic technique significantly complicates the decryption process for attackers or unauthorized entities, hence offering an additional level of security.
- ➢ The development of an effective image encryption model utilizing a heuristic technique significantly complicates the decryption process for attackers or unauthorized entities, thereby offering an additional level of security.

- The goal of this ISEO implementation is to save memory and processing time during the A-2DLCE-based encryption phase by improving how we choose the best keys during this stage.
- To maximize efficiency in terms of time and memory capacity, optimize essential characteristics to encrypt the secret picture from unauthorized individuals using A-2DLCE-based encryption.
- In order to enhance the model's visual quality, it is necessary to employ a tamper localization and recovery approach that efficiently identifies the tamper blocks.
- The objective of this performance evaluation is to compare the proposed image encryption model against both traditional methods and heuristic algorithms.
- The A-2DLCE model's parameters, such as level and filter length, may be fine-tuned with the help of the ISEO algorithm to lower the MSE and the encryption key can be optimized to save both memory and time during encryption. Resolving concerns around over-fitting is achieved by modifying the variables. Variable optimization helps to reduce the risk of over-fitting.

Image authentication has gained increased attention as a means of security due to its growing importance in several domains. However, it may be problematic now since it may incorrectly detect watermarks or the quality of the photographs may be poor. The unique security and privacy concerns of individuals and IP holders must be carefully considered in this context. It is imperative that individuals do everything that is required to stop imposters from using their personal images in an improper way. Consequently, several methods for detecting tampering and confirming authenticity have been developed via previous research.

The remaining sections are structured as follows. The Proposed Image Security Model for Encryption and Decryption is detailed in Section 2. In Section 3, presented the proposed Secure Image Encryption Method for Detecting and Recovering Tampering, and the simulation results are analyzed. Section 4 presents the algorithm performance results. Finally, concluding remarks are given in Section 5.

2. The Proposed Image Security Model for Encryption and Decryption

Conventional image encryption methods, which depend on rounds of dispersion and confusion, provide inadequate security and performance. There is no improvement in cryptography strength or efficiency or any other problem with the existing image encryption techniques while applying a new approach. The huge dataset makes it hard for standard methods to hide the message. The traditional method has a lot of drawbacks, such storing files on the cloud and sending pictures. Using chaos-based algorithms to process encrypted photos in systems is hard. It's hard to keep information safe and confidential. People know that traditional solutions are hard to utilize and don't assist you make forecasts right away. There is reduced delay with cloud-hosted applications, which makes them work better. Figure 1 shows a diagram of the proposed picture encryption system that leverages tamper localization.

Images collected from various data sources are then fed into the ADTCWT, which separates the input image into images with high and low frequencies. The proposed ISEO lowers the MSE and enhances the encrypting capability of the ADTCWT architecture by optimizing the level and filter length. The watermarking process begins with transforming and recovering the low frequency using the Arnold scrambling method. In this case, the original images have the distribution properties of the secret data embedded in them via a watermarking approach. The watermarking process begins with transforming and recovering the low frequency using the Arnold scrambling method. In this case, the original images have the distribution properties of the secret data embedded in them via a watermarking approach. The Arnold scrambling method is used to transform and recover the high frequency before compressive sensing is performed. Sparse representations are utilized to implement compressive sensing (CS). The Inverse ADTCWT model is employed to derive the composite image from the watermarked and compressed images. The encrypted composite image is sent to the A-2DLCE algorithm. In this case, the implemented ISEO is utilized to choose the key that minimizes both memory size and time. The encrypted image is then deciphered using the A-2DLCE. The decrypted images are provided to the ADTCWT model. It once again separates its low-frequency and high-frequency images. This instance involves extracting the watermark from the low-frequency photos. Decrypting the recovered watermark picture using the inverse Arnold scrambling method is the initial step in doing tamper detection and recovery. The high-frequency picture is subjected to CS using inverse Arnold scrambling. The Inverse ADTCWT is then used to generate the original image from the encrypted high-frequency and low-frequency ones.

The proposed picture encryption model outperforms other methods in terms of security and reliability.

2.1 Proposed ISEO

The original Social Engineering Optimizer (SEO) is a single-solution attacker/defender system. ISEO improves it by adding lightweight re-training/response operators and a quality-controlled initialization (via a short Sine-Cosine Algorithm, SCA, sweep). This makes it easier to repeat over hard terrain and, based on experience, makes early stalling less likely. The proposed image encryption with a tamper localization model makes use of the installed ISEO to improve communicated data security and successfully conceal the sensitive information. In the encryption based on A-2DLCE, the key is optimized. It is applied to lessen the problem of computational complexity. The encryption model that is based on A-2DLCE takes advantage of the implemented ISEO. The A-2DLCE-based encryption phase uses a binary format to choose the key, which helps reduce the amount of memory and calculation time. The present Social Engineering Optimizer (SEO) is modified to create the ISEO approach. Among the advantages of SEO algorithms is their capacity to improve the effectiveness and efficiency of social media marketing tactics. In order to find problems and assist in solving them, it may analyze patterns and behaviors. However, there are several shortcomings in the current optimization methods, such as Single Candidate Optimizer (SCO) [18], Red Fox Optimization (RFO) [19], and Golden Eagle Optimizer (GEO) [20]. There is also the possibility that it might be utilized for evil, especially in cases when other people's trust could be exploited or abused. Taking into account the pros and downsides, we used both traditional SEO and a new ISEO to tweak the ADTCWT system's settings to decrease the MSE and the A-2DLCE system's encryption key to speed up processing and use less memory.

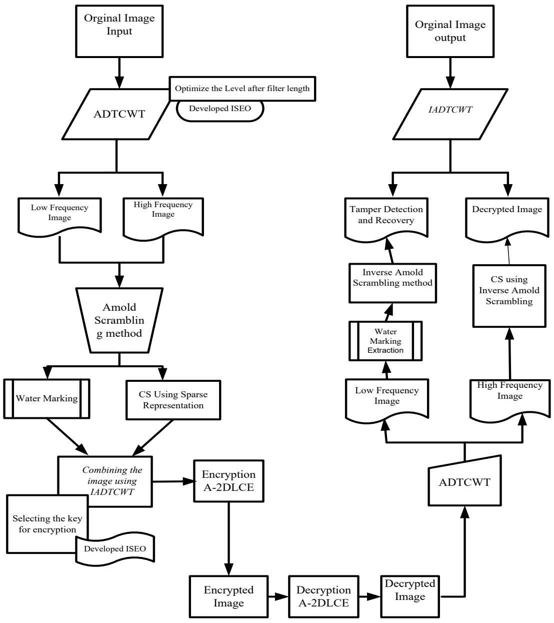


Figure 1: A schematic illustration of the proposed image encryption model employing tamper localization

The ISEO algorithm is a new kind of single-solution approach that has been developed to solve optimization problems with many goals, major engineering problems, and many benchmark functions. Complex and large-scale technological difficulties can be helped by the ISEO algorithm. This algorithm works better than other well-known and recently-developed metaheuristics, according to the results. The principal aims of this algorithm are its ease of development and its provision of easy procedures for parameter tweaking. Optimization of the parameters increases the likelihood of picking the right strategy. The method is employed to enhance the performance of deep learning models by adjusting their parameters. By supplying the best possible parameter values, the technique solves the problems of overfitting and scalability.

The stochastic, non-contractive dynamics of SEO and its advanced variant ISEO exemplify metaheuristic frameworks; nonetheless, guaranteeing deterministic convergence to a global optimum necessitates additional assumptions. According to the No-Free-Lunch (NFL) theorem for optimization, it is impossible to guarantee the same level of performance on all objective landscapes. Also, the baseline SEO/ISEO design doesn't have any built-in rules like vanishing step sizes, explicit cooling schedules, or ergodicity requirements that are usually needed for classical almost-sure convergence outcomes for stochastic search algorithms. Therefore, whereas restart techniques and parameter scheduling might enhance empirical convergence, the theoretical assurances are still constrained to probabilistic limitations under these conditions.

2.2 Digital Image Decomposing with ADTCWT

The Proposed ADTCWT-based image decomposition model receives data from the datasets. As compared to its rivals, the developed model performs better at separating the input pictures' low- and high-frequency components. The expected ADTCWT system also employs the suggested ISEO approach to tune parameters like level and filter length in order to decrease the MSE. Finally, the developed ADTCWT model produces LP_p^{High} and HF_p^{Low} images, respectively. The objective function VT_{FN} may be expressed as (1) for an image decomposition system that uses ADTCWT.

$$VT_{FN} = \underset{\{TG_Q^V, YB_R^Y\}}{\arg\min}(ME_{Ty}) \tag{1}$$

Equation (2) provides the mathematical form for the mean squared error (METV) in this context. In the interval [2 20] and [10,100], $TG^V{}_o$ and $YB^Y{}_R$, respectively, denote the level and filter length.

$$ME_{Ty} = \sum_{R}^{1}(FTG_{Lk}^{Rt} - DCD_P^{DF}) \tag{2}$$

In this case, R and DCDDFP set the total and decomposed image counts, respectively

2.3 Low and High frequency Image Processing using Arnold scrambling

A. Low Frequency Image Processing

The Arnold scrambling model processes low-frequency images. Subsequently, low-frequency LP_p^{High} images are employed to incorporate the watermark. In this context, watermarking [21] refers to the application of a mark on a low-frequency picture that may be either visible or hidden. It may consist of a textual composition, a symbol, or a visual representation. Watermarking the low-frequency image makes the encrypted data safer and more trustworthy. It stops tampering or illegal usage and helps prove ownership. So, a strong and safe mechanism keeps low-frequency photos safe. As a result, the images can be traced back to their real owner because they are always encrypted. The final result PGh_B^{Low} is a unique watermarked low-frequency image. To assess how smoothly the changes take place, it looks at the overall brightness and low frequencies of an image. It gets rid of a lot of noise also.

B. High Frequency Image Processing

The Arnold scrambling model is fed the obtained high-frequency images HP_P^{Low} [22] as input. It is possible to apply the Arnold transform, which changes pixel supervisors, to digital images.

$$\begin{bmatrix} c' \\ d' \end{bmatrix} = \begin{bmatrix} kl \\ mn \end{bmatrix}\begin{bmatrix} c \\ d \end{bmatrix} \left| R, c, d \in \{0,1,.,..R-1\} \right| \tag{3}$$

For displaying an image in a matrix format using the Arnold transform, Eq. (3) can be used. In the original image, the coordinates are (c,d), and in the modified version, they are (c',d'), which is the same as the original image's coordinates. To complete an Arnold transform, each raster in an R×R picture must have been subjected to Eq. (4). By utilizing the transformation approach, one may apply an Arnold transform to an R×R scaled image on several instances. A more generalized transformation that may do the same thing as the Arnold transformation was subsequently discovered by someone utilizing Eq. (5).

$$\begin{bmatrix} c' \\ d' \end{bmatrix} = \begin{bmatrix} kl \\ mn \end{bmatrix}^{o}\begin{bmatrix} c \\ d \end{bmatrix} \left| R, c, d \in \{0,1,.,..R-1\} \right| \tag{4}$$

$$\begin{bmatrix} c' \\ d' \end{bmatrix} = \begin{bmatrix} kl \\ mn \end{bmatrix}^{L}\begin{bmatrix} c \\ d \end{bmatrix} \left| R, c, d \in \{0,1,.,..R-1\} \right| \tag{5}$$

As a consequence, the watermark system can extract and store the contents of the watermark within a key form, making the data more secure. The Arnold transform is a cyclic transformation that involves repeatedly scrambling an image to restore it to its original condition. Finally, the high-frequency images are transmitted to the CS process using the Arnold scrambling model once the sparse representation has been used. The original data can be reliably reproduced with a small number of observations. Both sampling and reconstruction are provided by the encoder and decoder, which are the two main components of compressed sensing.

3. The Proposed Secure Image Encryption Method for Detecting and Recovering Tampering

A. Image Encryption with Developed A-2DLCE

The images are encrypted using A-2DLCE. The private key is generated by the logistic map, which also supplies a random sequence. This 2D logistic chaotic system-based picture encryption offers substantial unpredictability, high key sensitivity, and minimal pixel correlations. The conventional framework employs a network that uses permutations and substitutions. The proposed developed A-2DLCE image encryption from a structural perspective is depicted in Fig 2.

The 2D logistic map is evaluated according to Equation (6).

$$2Dmap = \left\{ \begin{matrix} y_{j+1} = s(3z_j + 1)y_i(1 - y_j) \\ z_{j+1} = s(3y_{j+1} + 1)z_j(1 - y_j) \end{matrix} \right\} \qquad (6)$$

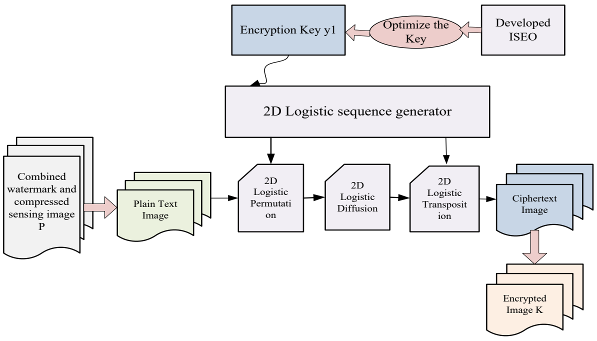


Figure 2: A-2DLCE-based image encryption

where constant value is represented by s, and j keeps track of the number of iterations.

Images featuring watermarks at low frequencies are denoted by w_e^L and photos demonstrating compression at high frequencies are represented by C_r^H . The ADTCWT model processes these images using the inverse decomposition method to get the composite image. The decomposed picture sub-band sizes are equal to the original image sizes and give the invariant measurements for ADTCWT. It merges the quantity of sub-bands. In the inverse of the ADTCWT process, some low-frequency and high-frequency coefficients are mixed. For encryption, the merged image is passed to the A-2DLCE-based algorithm. Here, the binary key is selected using the implemented ISEO to minimize computation time and memory space from A-2DLCE-based encryption. It offers negligible pixel correlations and robust key sensitivity for data processing and execution. Nonetheless, other issues persist, including uneven distribution, insufficient parameter space, and inadequate security. Mitigating the hazards associated with data management is almost unattainable, and the implementation incurs substantial costs. A private key-based encryption method utilizing A-2DLCE was employed to secure the data. The goal function, as defined in Eq (7), aims to minimize both time and memory use.

$$Ob_f = \underset{\{yl\}}{\arg\min}\,(Time + M\_Size) \qquad (7)$$

In this case, the optimal key is yl, which falls within the interval [0, 1]. The memory size is called M_size, and time is represented by Time. To improve performance, the real implementation time is calculated by minimizing memory size and time. Equation (8) is used to determine the computation time.

$$Time = \frac{1}{Oq} + \frac{N_j}{u_j} \qquad (8)$$

In this case, Nj indicates the message size, while Oq represents the total number of messages. As a crucial metric for encryption, the computation time of the term uj has a direct impact on the encryption performance. According to Eq. (9), the size of the memory is

$$M\_Size = PO_s \times Ws \qquad (9)$$

The size of the message is denoted by Ws, while its position is determined by PO$_s$. Memory size for encryption is denoted by the word M_Size. The last encrypted picture is recorded by $k^N{}_t$. Figure 7 displays the designed A-2DLCE image encryption from a structural perspective.

B. The A-2DLCE Image Decryption and ADTCWT Separation

The image may be decrypted using the private key using the A-2DLCE. Upon completion of the encryption phase, $K^N{}_t$ informs the A-2DLCE-based decryption process of the finalized encrypted image. Decryption is a process that reverses encryption; it use a logistical chaotic map to decode the encrypted picture by picking a one-dimensional pixel value from the interval [0, 1]. The principal function is to convert ciphertext into plaintext. The decryption process is defined by Equation (10)

$$E_k^D = D_k \oplus (y1, z1) \tag{10}$$

In this case, the key sequence is represented by the phrase y1, z1. Dk is the value of a pixel in a one-dimensional space. The ADTCWT model is provided with the decrypted image $P^{C}{}_{i}$. It divides the images into two parts, with one for low-frequency and one for high-frequency.

C. Tamper Localization Process on Low-frequency Images: Extracting Watermarks

The watermark extraction procedure takes the decrypted low-frequency images as input. The process of removing or decoding an image's watermark is called watermark removal. A watermark is a common way to protect intellectual property or to show who owns an image and stop others from using it without permission. The low-frequency component employs watermarks for restoration and tamper detection, while the high-frequency section additionally contains a watermark. This watermark is transmitted via an encrypted channel to establish its unique authentication significance and to identify any interference. It can detect tampering and surrounding bricks. The color forecasting technique takes the modified pixels as input. The pixel projection method is followed by making use of the original pixel. Next, the tamper localized method is used to identify the tamper components. The objective of tamper detection is to enhance the clarity of the image. Following this procedure, LP_p^{Low} notes the extracted watermark from the low-frequency pictures.

D. Analysis of High-frequency Images using Inverse CS and Decryption

The General Procedures for the Developed Image Security Model. The inverse CS phase is applied to the decrypted high-frequency images DN_T^{High}. The inverse processes of CS took place here, and their result was the high-frequency image HP_p^{IG}.

E. Acquisition of Original Images with the assist of Inverse ADTCWT

The original image acquisition model, which is based on inverse ADTCWT, is fed with low-frequency watermark images and high-frequency images that are derived using inverse CS. The resultant FTG_{Lk}^{Rt} consists of the original photos, which are produced by the inverse ADTCWT model that processes the high-frequency and low-frequency images.

4. Results and Analysis

In the experimental examination of the proposed image encryption system, it was performed in a Python environment. The optimal parameters for the image decomposition and encryption phase were a population of 10, a maximum iteration of 50, and chromosomal lengths of 50 and 16, respectively. Several models and algorithms were utilized for the comparison process to validate the effectiveness of the designed ISEO-A 2DLCE approach. These included A-2DLCE, Chaotic maps, and DWT as well as optimization strategies such as SEO, SCO, and GEO.

Performance Metrics:

$$MSE = \frac{1}{k}\sum_{j=1}^{k}\left(x_i - Tx_{j-1}\right)^2 \tag{11}$$

$$NPCR = \frac{\sum_{j,k} E(j,k)}{X \times I} \times 100 \tag{12}$$

$$PSNR = 10\log_{10}\left[\frac{S^2}{MSE}\right] \tag{13}$$

$$SSIM = \frac{2\lambda y \lambda z}{\lambda_y^2 + \lambda_z^2}\frac{2kyz}{k_y^2 + k_z^2} \tag{14}$$

$$UACI = \frac{1}{X \times I}\left(\sum_{j,k}\frac{|D(j,k) - D(j,k)|}{255}\right) \times 100 \tag{15}$$

4.2 Outcomes obtained from the Proposed Security model

The following database, https://www.kaggle.com/datasets/adityamahimkar/iqothnccd-lung-cancer-dataset, has the photos needed to carry out the procedure of the produced encryption prototype. There are 1,190 pictures in the collection, which include fragments of CT scans from 110 distinct patients. There are three primary groups of tumor-related data: normal, benign, and malignant. People think that 55 of them are healthy, 15 of them are not hazardous, and 40 of them have cancer. Figure 3 shows what happens to analyzed, watermarked, encrypted, decrypted, and watermarked images when the suggested approach is used.

4.3 Evaluation Analysis of the Proposed Image Security Model

Figure 4 shows the results of comparing the developed picture security method to other heuristic methods and conventional techniques. Various error measures are used to validate the constructed model, with picture size being the primary metric. It improves the sensing and picture encryption procedure while simultaneously decreasing error rates. Compared to GEO-A-2DLCE, SEO-A-2DLCE, and SCO-A-2DLCE, the derived ISEO-A-2DLCE model outperforms them with MSEs of 38.57%, 32.57%, 94.5%, and 23.67%, respectively, while evaluating images with a resolution of 1024 × 1024; and also achieving better results of other metrics in terms of PSNR, SSIM, UACI and NPCR. The proposed image security structure was tested using the image sizes, and the results are better.

4.4 Examining the Proposed Model's Computational Time

The analysis of computation time and memory consumption on the proposed security model is shown in Figures 5. Processing time and memory utilization partially determine the efficiency and speed of an encryption technique. This data enables us to understand how long it takes to encrypt an image and how much memory is required during the process. From the Fig 5(a), the proposed ISEO-A-2DLCE model is 28%, 35.92%, 62.5%, and 52.85% more effective in terms of computational time Superior performance was achieved by the security-aware image encryption system based on ISEO-A-2DLCE in comparison to prior systems in terms of computational time and small memory size. The outcome showed that the recommended solution is very effective at reducing energy and computational overhead and is speedy, enabling the encryption of massive volumes of data quickly.

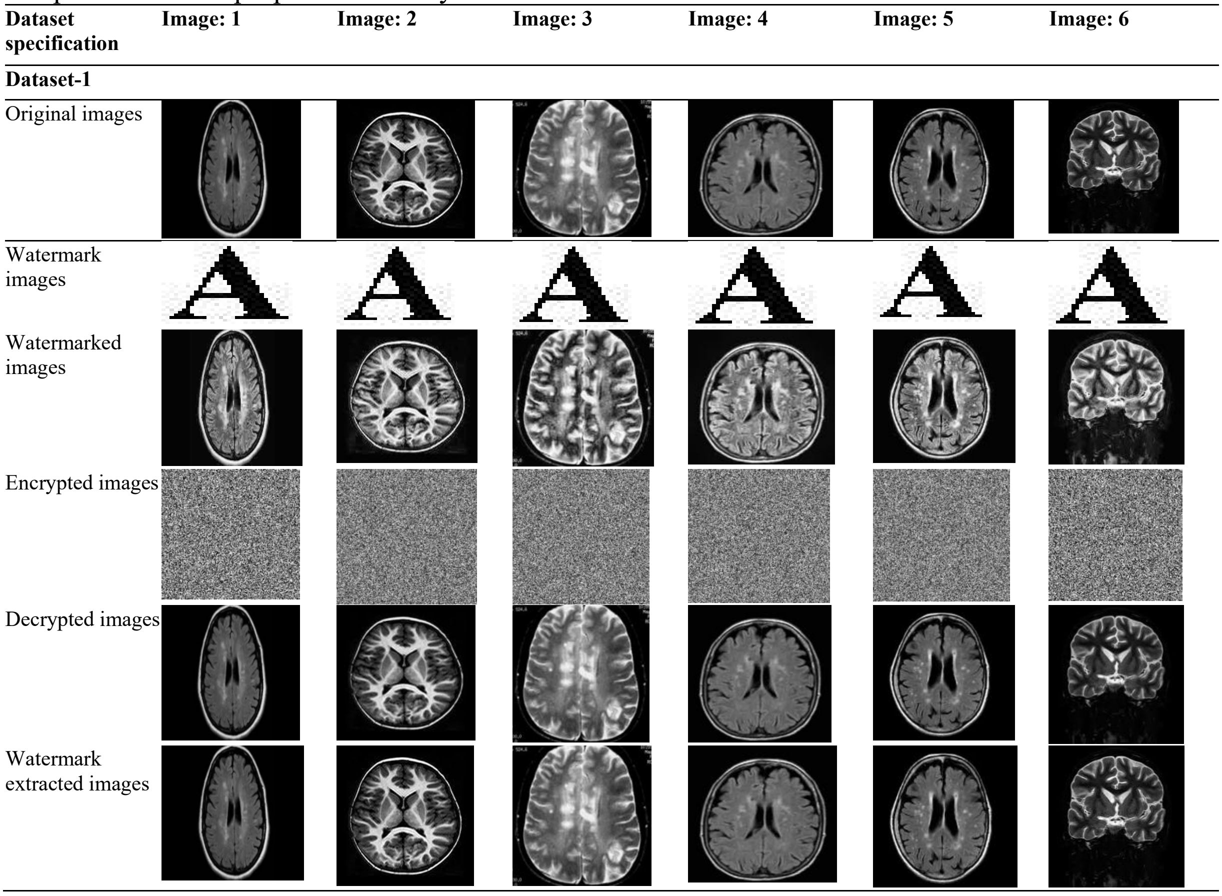
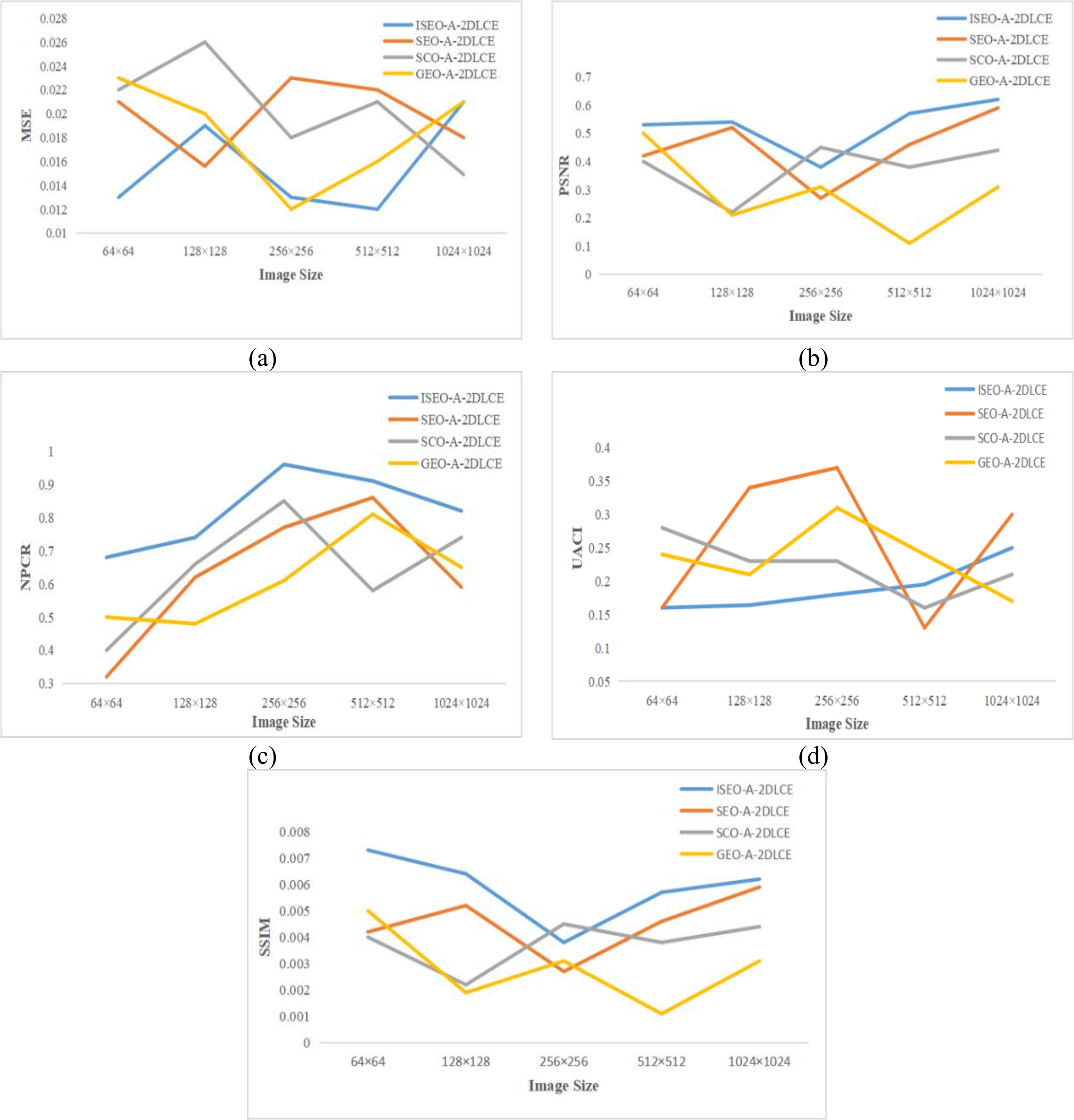


Figure 3: The Proposed Encrypted model finding

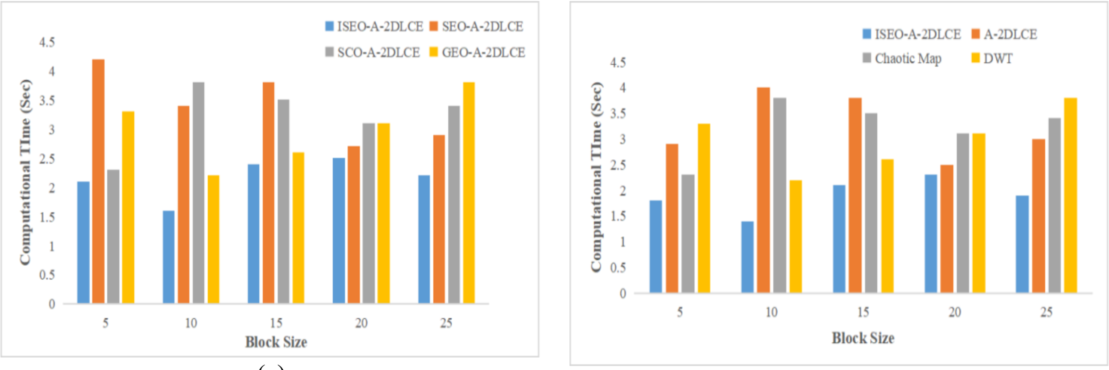


(a) (b)

(c) (d)

(e)

Figure 4: Evaluation of the Proposed Method with (a) MSE, (b) PSNR, (c) NPCR, (d) UACI, and (e) SSIM



(a) (b)

Figure 5: Evaluation of the suggested security encryption system's performance using computational time with different techniques

Conclusion

This paper presents a new encryption approach that puts optimization first. The suggested strategy made sure that picture encryption was safe and reliable by changing key methods and encryption models so that images couldn't be changed. The new ADTCWT paradigm protects data transport and encrypts pictures. The scene can be broken up into its easiest and hardest levels using the ADTCWT model. Later, the A-2DLCE type secured the photos. Key part of this project is using encryption to keep private information from people who want to see it. One of the beneficial things about the recommended strategy for image encryption was that it made it safer to produce, share, and store keys. The application made it such that no one could edit or interfere with the data without authorization. When the level and filter length were modified, the ADTCWT structure performed best for the new ISEO. The developed ISEO algorithm's parameters may be fine-tuned to effectively produce the optimal response. To conclude, the proposed A-2DLCE model was tested with several performance metrics to see the manner in which it performed. With respect to the UACI metric, the created model outperformed GEO-A-2DLCE, SCO-A-2DLCE, and SEO-A-2DLCE by 13.46%, 21.67%, 11.4%, and 1.39%, respectively. The results proved that the proposed image security model preserved encrypted data with a high degree of robustness, which was useful for several applications.

References

[1] Zhang, R., & Xiao, D. (2020). A secure image permutation–substitution framework based on chaos and compressive sensing. International Journal of Distributed Sensor Networks, 16(3), 1550147720912949.

[2] Xiao, D., Zhao, A., & Li, F. (2022). Robust watermarking scheme for encrypted images based on scrambling and Kronecker compressed sensing. IEEE signal processing letters, 29, 484-488.

[3] Saravanan, N., Muthukumaran, K., Nandhini, T., Shabeen, S. S., Sasikumar, G., & Yasar, I. M. (2025, April). A Novel Approach to Audio-Based Emotion Recognition Using Transfer Learning Algorithm (Wav2Vec2. 0). In 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 539-543). IEEE.

[4] Thabit, R., Al-Askari, M. A., Mohammed, D. Z., Anaam, E. A., Mahmood, Z. H., Jabbar, D. J., & Salih, Z. A. (2025). Face image authentication scheme based on MTCNN and SLT. Multimedia Tools and Applications, 1-43.

[5] Wang, C., Zhang, Q., Wang, X., Zhou, L., Li, Q., Xia, Z., ... & Shi, Y. Q. (2025). Light-Field Image Multiple Reversible Robust Watermarking Against Geometric Attacks. IEEE Transactions on Dependable and Secure Computing.

[6] Shi, H., Yan, K., Geng, J., & Ren, Y. (2024). A cross-embedding based medical image tamper detection and self-recovery watermarking scheme. Multimedia Tools and Applications, 83(10), 30319-30360.

[7] Capasso, P., Cattaneo, G., & De Marsico, M. (2024). A comprehensive survey on methods for image integrity. ACM Transactions on Multimedia Computing, Communications and Applications, 20(11), 1-34.

[8] Liu, Z., & Xue, R. (2024). Visual image encryption based on compressed sensing and Cycle-GAN. The Visual Computer, 40(8), 5857-5870.

[9] Ping, P., Yang, X., Zhang, X., Mao, Y., & Khalid, H. (2022). Generating visually secure encrypted images by partial block pairing-substitution and semi-tensor product compressed sensing. Digital Signal Processing, 120, 103263.

[10] Qi, Y., Bi, J., Peng, H., & Li, L. (2024). Efficient Homomorphic Encryption for Multi-key Compressed Sensing in Lightweight Cloud-based Image Processing. IEEE Sensors Journal.

[11] Lu, J., Wang, T., & Zhang, J. (2024, November). A color image channel fusion encryption scheme combining a four-dimensional chaotic system. In 2024 2nd International Conference

on Computer, Vision and Intelligent Technology (ICCVIT) (pp. 1-9). IEEE.

[12] Shuo, Z., Pijun, H., Yongguang, C., & Wang, B. (2023). A visually secure image encryption method based on semi-tensor product compressed sensing and IWT-HD-SVD embedding. Heliyon, 9(12).

[13] Shi, Y., Chen, R., Liu, D., & Wang, B. (2023). A visually secure image encryption scheme based on adaptive block compressed sensing and non-negative matrix factorization. Optics & Laser Technology, 163, 109345.

[14] Zhang, R., Xiao, D., & Chang, Y. (2018). A Novel Image Authentication with Tamper Localization and Self-Recovery in Encrypted Domain Based on Compressive Sensing. Security and Communication Networks, 2018(1), 1591206.

[15] Xue, W., Luo, C., Shen, Y., Rana, R., Lan, G., Jha, S., ... & Hu, W. (2020). Towards a compressive-sensing-based lightweight encryption scheme for the internet of things. IEEE Transactions on Mobile Computing, 20(10), 3049-3065.

[16] Pankaj, S., & Dua, M. (2024). Chaos based medical image encryption techniques: A comprehensive review and analysis. Information Security Journal: A Global Perspective, 33(3), 332-358.

[17] Shao, J., Bai, E., Jiang, X., & Wu, Y. (2024). Multi-View Light Field Images Compression and Encryption Using Enhanced 3D Chaotic System and Pixel-Bit-Scrambling. IEEE Access.

[18] Shami, T. M., Grace, D., Burr, A., & Mitchell, P. D. (2024). Single candidate optimizer: a novel optimization algorithm. Evolutionary Intelligence, 17(2), 863-887.

[19] Mohammed, H., & Rashid, T. (2023). FOX: a FOX-inspired optimization algorithm. Applied Intelligence, 53(1), 1030-1050.

[20] Mohammadi-Balani, A., Nayeri, M. D., Azar, A., & Taghizadeh-Yazdi, M. (2021). Golden eagle optimizer: A nature-inspired metaheuristic algorithm. Computers & Industrial Engineering, 152, 107050.

[21] 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.Bhatti, U. A., Yu, Z., Li, J., Nawaz, S. A., Mehmood, A., Zhang, K., & Yuan, L. (2020). Hybrid watermarking algorithm using Clifford algebra with Arnold scrambling and chaotic encryption. IEEE Access, 8, 76386-76398.

[22] Bhatti, U. A., Yuan, L., Yu, Z., Li, J., Nawaz, S. A., Mehmood, A., & Zhang, K. (2021). New watermarking algorithm utilizing quaternion Fourier transform with advanced scrambling and secure encryption. Multimedia Tools and Applications, 80(9), 13367-13387.

[23] Loan, N. A., Hurrah, N. N., Parah, S. A., Lee, J. W., Sheikh, J. A., & Bhat, G. M. (2018). Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. IEEE Access, 6, 19876-19897.

[24] Attaullah, Shah, T., & Jamal, S. S. (2020). An improved chaotic cryptosystem for image encryption and digital watermarking. Wireless personal communications, 110(3), 1429-1442.

[25] Chen, Y., Jia, Z., Peng, Y., & Peng, Y. (2023). Efficient robust watermarking based on structure-preserving quaternion singular value decomposition. IEEE Transactions on Image Processing, 32, 3964-3979.

[26] Jiang, M. R., Feng, X. F., Wang, C. P., Fan, X. L., & Zhang, H. (2023). Robust color image watermarking algorithm based on synchronization correction with multi-layer perceptron and Cauchy distribution model. Applied Soft Computing, 140, 110271.

[27] Zhang, H., Li, Z., Liu, X., Wang, C., & Wang, X. (2022). Robust image watermarking

algorithm based on QWT and QSVD using 2D Chebyshev-Logistic map. Journal of the Franklin Institute, 359(2), 1755-1781.

[28] Dong, Y., Yan, R., & Yin, C. (2024). An adaptive robust watermarking scheme based on chaotic mapping. Scientific Reports, 14(1), 24735.

[29] Wu, W., Dong, Y., & Wang, G. (2024). Image Robust Watermarking Method Based on DWT-SVD Transform and Chaotic Map. Complexity, 2024(1), 6618382.