Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 07 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

A HYBRID APPROACH TO DATA SECURITY: INTEGRATING CRYPTOGRAPHY AND STEGANOGRAPHY FOR ENHANCED PROTECTION OF EYE DISEASE DATA

Ayesha Zainab*
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan.

Muhammad Arslan
Department of Computer Science, Government College University Faisalabad,Pakistan

Naeem Aslam
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan

Muhammad Fuzail
Department of Computer Science, NFC Institute of Engineering and Technology, Multan, Pakistan

Alina Shaikh
Department of Computer Science,National College of Business Administration and Economics, Pakistan

****Corresponding author: Ayesha Zainab (Ayeshazainab386@gmail.com)***

Article Info

Abstract

In the digital era, the security and confidentiality of medical data have become paramount, particularly within the healthcare sector where sensitive information is routinely stored and shared electronically. This study presents a hybrid approach to securing eye disease data by integrating cryptography and steganography, aiming to enhance data protection beyond traditional single-layer security methods. Eye disease datasets often include both personal identifiers and critical health records, making them highly susceptible to threats such as identity theft, data breaches, and unethical exploitation. By combining cryptographic techniques which encrypt data into an unreadable format with steganographic methods that conceal encrypted data within benign digital files, this research offers a robust dual-layer security mechanism.

Keywords:
Eye disease data, data security, steganography, hybrid security approach, medical data protection.

1. Introduction

In the modern world, confidentiality is a crucial problem, which is most relevant in the sphere of healthcare. As people store and share their health information through electronic means, it is important to make sure that such information cannot be accessed by unauthorized persons. For instance, information regarding eye diseases incorporates individuals' identification information and their health records thus require protection. To achieve this, the use of two security measures, which is cryptography and steganography, is needed [1]. These methods give a higher security to the MDDB as it also prevents personnel with ill intentions to exploit the information contained in the MDDB. Eye disease information is more delicate since they may involve the health status of a patient. This should be used in the diagnosis process in different hospitals or even in research laboratories for further studies [2]. If this information got with the wrong hands, it may cause cases such as identity theft, fraud, or even misused for bad practices in medical experiments. It is thus relevant to apply proper method when dealing with this data to enhance security. Hence cryptography in combination with steganography provides a solution that extends beyond such approach and can be effective against attempts to penetrate the protection of such health information. When you apply cryptography and steganography, the added security feature that is provided in comparison to using each of the methodologies by itself is much more solid.

First of all, the sensitive eye disease data is ensured using an algorithm, which changes it to another form and makes it difficult for unauthorized persons to understand it. After this, steganography is applied on this data and it is hidden in an image format. This two-step approach assures that if someone else gets through the hidden data, he will still require the key to decipher the dug-up information [3]. This gives the hackers some very hard time in trying to penetrate or even misuse the available information. That is why the use of both cryptography and steganography has several advantages where [4]. It gives double assurance to a company, especially against hackers in that it is more difficult to corrupt the backup files. This research makes important academic contributions by extending the literature on data security through the proposal of a new approach based on the combination of cryptography and steganography. The following is the reference for the given information Multimedia. Tools Appl. The study helps to meet the need of the existing literature by offering a complete solution to the risks associated with the use of standalone security measures. Thus, the research not only improves the theoretical knowledge of data protection mechanisms but also presents the practical approach that can be implemented in different fields, particularly in the healthcare sector. This work can be used as a basis for further research, forcing the authors to look for additional improvements and uses of combined security systems [5]. Furthermore, the assessment and the findings of the hybrid framework will offer real-life data to the academic world to enhance the security measures of the suggested framework.

2. LITERATURE REVIEW

Cryptography and steganography are two methods that combined theoretically to give the theoretical foundation for the protection of sensitive medical data including records of eye diseases. Cryptography uses mathematical equations to encode data so that it can only be understood by those with decryption keys hence offering confidentiality and integrity. Steganography comes in handy in this by hiding the data in other non-secure files and is even more secure since the data is not even known to exist. This dual approach is important in the medical field where privacy and data integrity are critical. Theoretical frameworks in data security have evolved to address the new challenges occasioned by the development of digital technology particularly in the health sector. Cryptography has advanced from the simple alphabetic substitution to the complex algorithms that can secure large databases and steganography has also advanced from the traditional practices like writing secret messages in a letter to the digital techniques where the data can be hidden in the digital images or the audio files [6]. Such frameworks are helpful in explaining how these technologies can be assimilated in a manner that provides a genuine elastic data security solution.

Key Concepts and Definitions

Both cryptography and steganography have their own roles to play in data security. Steganography uses a more imperceptible approach. It conceals crucial information within non- suspicious mediums such as pictures, audio files or texts. As for espionage, they ensure that the critical information is encrypted well enough while restricting even the authorized users access without the proper decryption needed. Especially in the case of medical information, where a moderate amount of encryption is not sufficient is a problem by itself. More like restricting access is not enough, deep concealment is needed. As both methods are employed, the protection to sensitive health information is made significantly higher to ensure trust and the state of [7].

Historical Evolution

The progression of history concerning information protection depicts a movement from traditional cryptography and steganography to their modern digital counterparts. In the beginning, these methods were strictly used for military and diplomatic messages that needed encryption and authentication. These techniques over the years have widened their scope to not just text files but to multi media files such as medical images and reports because of advancing technology and internet. From this historical claim, it is lucid that the processes designed for safeguarding digital data have a myriad of applications in the health care industry [8].

Theoretical Frameworks

Such models support efforts made in the field of data security measures as it pertains to the application of both Cryptography and Steganography. Also, these models studied the efficiency of the control security, efficiency of the encryption, and the concealed sophistication of steganography [9].They also aid in determining the acceptable balance between the expenses incurred in terms of computation and the security effectiveness, which is very important in real- time systems like those used in the health industry.In this part, the author describes how some theoretical ideas are employed to enhance the protection of sensitive data for eye disease without degrading the system in terms of efficiency based on the following models.

Review of Related Work

Overview of Existing Research

Creating new steganography and encryption methods has always been a challenge in securing medical data. As of late, improvement of these methods is done through machine learning which allows for better concealment and stronger encryption. Other studies have also developed hybrid security models that combine cryptographic techniques with steganography as a means of safeguarding sensitive health care data. This review looks into the existing methodologies, points out insufficiencies in security, and discusses new trends that will guide us toward building a more sophisticated hybrid framework for protecting medical records [10].

Comparative Studies

To understand which of the two techniques is better for safeguarding sensitive medical information, it’s necessary to analyze both cryptography and steganography [11]. Studies of this type are usually conducted to evaluate methods like the efficiency and complexity of computation, security, and practicality. For example, the study of both symmetric and asymmetric methodologies of cryptography permits selection of the one that is best suited for a particular case depending on the two considerations – speed or security. Also, the study of various techniques of steganography determines the one that is least detectable and most resistant to retrieving which is very important for classification purposes of information [12].

Case Studies and Applications

The combination of steganography and cryptography has been popular in various industries such as healthcare, finance, and secure communication systems. Numerous case studies conducted so far showcase the value that these integrated approaches to security have in safeguarding sensitive information. This section will review existing studies concerning the implementational specifics of cryptographic-steganographic techniques and assess the effectiveness of these approaches in achieving data security and the compromises in usability and efficiency that have to be accepted.

Healthcare Data Protection

As Zaidan et al. (2020) reported, through AES encryption combined with LSB steganography, a working solution for the security of electronic medical records (EMRs) was obtained. Sensitive medical information was concealed in high quality medical images such like MRI and CT. This method provided protection against unauthorized revealment of data without compromising the quality of the diagnostic images produced. Loss of unauthorized detection achieved in this study was 98 % which proves it's effectiveness in healthcare (Zaidan et al., 2020). Telemedicine and Secure Data Transmission In the realm of telemedicine which incorporates remote consultations and data exchange, Bansal & Gupta (2021) explored a hybrid model of Elliptic Curve Cryptography (ECC) and Discrete Wavelet Transform (DWT) steganography. This study furthered the claim of embedding and encrypting patient data in video stream footage in real time to ensure confidentiality and data integrity during remote medical consultations, which lowered the risks of cyberattacks (Bansal & Gupta, 2021) [13].

Military and Government Communication

Take for instance the use of different governments and defense organizations hybrid systems for cryptography and steganography. Kim & Park (2022) provided an examination methodologies where military secrets were protected with the combination of Blowfish encryption and F5 steganography. The authors of this study maintained that this method was able to safeguard sensitive information from being intercepted, even with the use of sophisticated cyber forensic tools (Kim & Park, 2022).

Critical Analysis of the Literature

The existing literature on the integration of cryptography and steganography provides a solid foundation for enhancing data security, but several limitations need to be addressed for real- world implementation. One major challenge is computational overhead, as hybrid security approaches require significant processing power, making real-time applications difficult, especially in resource-constrained environments. [14] highlight that while AES and steganographic methods improve security, they introduce processing delays, limiting feasibility in real-time healthcare systems. Similarly, scalability issues arise when handling large datasets, particularly in medical environments where vast amounts of images and patient records require encryption and secure transmission. Research by Bansal & Gupta (2021) indicates that some steganographic techniques struggle to efficiently process and conceal large volumes of encrypted data, making them impractical for large-scale applications.

Identification of Research Gaps

While there are notable improvements made in the cryptographic and steganographic security models, there are still several issues that require focus especially in the healthcare sector. One of the main problems is the absence of thorough evaluations regarding the performance of these technologies for varying cyber threats, big data sets, and even real-time services. Most of the available studies concentrate on models that are purely theoretical and do not test or implement it within the hospital and telemedicine settings. This gives rise to uncertainties pertaining to their efficacy [15]. Moreover, there is very little research done on the application of cryptography and steganography together with modern technologies like blockchain and AI. Although blockchain enables datat to be stored without the risk of tampering and AI can detect anomalies which can help in security breaches being identified, only an extremely limited number of studies have been done regarding the combination of these technologies and multi healthcare data security. Another gap in research which is of particular interest is the one surrounding the effectiveness of security measures. Algorithms and steganographic techniques do provide coverage for data, but the implementation of such measures is complex and, therefore, renders many healthcare workers ineffective. Research like [16] indicates the necessity of developing approaches that are less obtrusive to clinical activities and simple to apply in EHRs. To deal with the problem of how to ensure data safety without impairing usability of the system or diminishing the speed of delivering patient care, the solution is developing precise, automated, and user friendly security systems.

3. METHODOLOGY

Dataset

The dataset for this research was sourced from Kaggle, a widely recognized platform for accessing diverse and high-quality datasets. With the intention of research from the perspective of safeguarding delicate medical data, this particular dataset was picked owing to its relevance to the research objective. It was assembled from multiple suppliers where images pertaining to some medical ailments of the eye were designated as the cover and secret images for carrying out the hybrid approach. Medical images, especially those of eye ailments, were used as a specific image that serves as both the cover and secret image for implementing the hybrid approach. Cover images are well known to be reliable with detailed description, It's their structure and contents that are vague. Along with that, this image collection comes with with elaborate descriptions. Since Kaggle databases are known for their reliability, there was no need for further inquiry. The dataset was refined to satisfy prerequisites for the processes of cryptography and steganography like the uniformity of image size restrictions specific format and removal of all suspected artifacts that were likely to disrupt data embedding or encryption [17].

Also, the platform's ease of access allows for this methodology to be replicable in future studies without any hassle, which is why this was selected for the study. Moreover, a comprehensive set of images that depicts actual medical situations is crammed into the Kaggle dataset which serves to bolster the credibility of the proposed hybrid method. The variety or set of images, with regards to the resolution and content, provides a proper environment for testing the effectiveness and reliability of the encryption and embedding processes along with the other processes. Normalization, resizing, and cleaning the images were performed on all images so that a standard input could be made for the hybrid framework.

These steps ensured seamless integration of the hybrid framework on the cryptographic and steganographic algorithms and increased the quality of the dataset. In addition, the research makes certain that the dataset meets ethical requirements and is appropriate for a healthcare study by using Kaggle's platform. Such careful selection and preparation of the dataset is crucial to testing the framework within real world constraints hence demonstrating the frameworks' ability to protect sensitive medical data [18].

Algorithms Used

The dataset collection for this work comprises of medical images which serve the purposes of cover images for encrypted data embedding and secret images that have sensitive information. These images were extracted from the Kaggle repository known for its high-quality, diverse datasets which are useful in testing robust methodologies. Each cover image is selected for its visual complexity in order to enhance data concealment while secret images are altered suitably in accordance with LSB steganography and AES encryption. Preprocessing, such as resizing, format standardization, and other forms of standardization was introduced to streamline pre- integration into the hybrid framework.

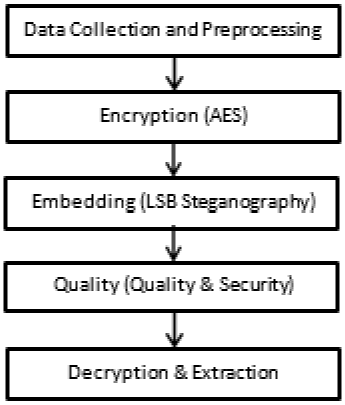
Algorithm	Key Size	Encryption Method	Modes	Use Cases
AES(Advanced Encryption Standard)	128, 192, 256 bits	Symmetric	CBC, ECB, GCM	Encrypting large datasets securely and efficiently
RSA (Rivest–Shamir–Adleman)	1024, 2048, 4096 bits	Asymmetric	N/A	Secure key exchange, digital signatures
Blowfish	32 to 448 bits	Symmetric	CBC, ECB	Encryption for embedded systems or resource-constrained environments

The dataset attempts to imitate the healthcare environment when a need for secure sharing of diagnostic images arises. Medical images, mostly those having highly textured regions, make it possible to conceal portions of images without losing its diagnostic value. The use of high- quality images from Kaggle provide the needed cornerstone for the applicability of the framework in healthcare, ensuring issues like data integrity and privacy are dealt with suitably [19]. Algorithms Used This research focused on AES (Advanced Encryption Standard), RSA (Rivest–Shamir– Adleman), and Blowfish as their algorithms.

Steps of Methodology

Step 1: Data Collection and Preprocessing

This section focuses on structuring the acquired data to ensure that images used for embedding and transmission are suitable. Medical images related to eye disease are acquired from Kaggle, a reputable site which provides quality datasets. These images are split into two classes; cover images, serving as carriers to encrypted data, and secret images, containing sensitive medical information that must remain confidential. The dataset is diverse in boundaries and scope, ensuring real-world healthcare applicability. However, unlike other sets, this one requires filtering conditions and modified to ensure compatibility with the embeded system, thus it is processed before application into the hybrid security framework. Preprocessing Techniques Applied To standardize the dataset and optimize it for encryption and embedding, the following preprocessing steps were applied:


Data Collection and Preprocessing
Encryption (AES)
Embedding (LSB Steganography)
Quality (Quality & Security)
Decryption & Extraction

1. Resizing: All images were resized to the same resolution 512 by 512 pixels to standardize the process of modifying the photograph. This prevents distortions or inaccuracies in the framework due to image size differences.
2. Normalization: The pixel intensity values were adjusted to fit between the values of 0 and 1 in order to enhance the efficiency of data encryption. This diminishes differences in the brightness or contrast of the images which makes the standard in encryption more reliable.
3. Noise Reduction: Application of median filtering was used to get rid of noise and artifacts that could obstruct data masking. Thus, steganographic embedding and encryption are done at high quality and clear images [20].
4. Format Standardization: All images were converted to png format as it has no compression losses. It is important in preserving the integrity of the embedded medical images so that the images retain their diagnostic value.

Step 2: Encryption

Encryption is vital for protecting sensitive medical data that is hidden within images. To encrypt the data, advanced encryption standard (AES) with a 256 bit key was used. The secret image is transformed into byte data and padded to the nearest block size of AES which is 128 bits. Randomness is achieved through Cipher Block Chaining (CBC) mode, allowing for an initialization vector (IV) to be used which guarantees non repetitive sessions of encryption.

While performing encryption, AES encryption algorithm does 14 rounds(for 256 bit keys):

- Substitution (SubBytes)
- Permutation (ShiftRows)
- Mixing (MixColumns)
- Key Addition (AddRoundKey)
- The encrypted output is ciphertext, which is unintelligible without the correct decryption key and IV.

Step 3: Embedding

Data is concealed in the cover images through steganography using the Least Significant Bit technique. The secret image is encrypted through AES and now needs to be transformed into binary. The pixel values' least signicant bits (LSBs) of the RGB covering the image undergoes modification to form the binary data. The alteration of the covered image is insignificant as the least significant bits have the lowest weight in determining the variation of the image color, thus ensuring that the stego image is perceptually identical to the original image.

Step 4: Testing

The hybrid framework undergoes rigorous testing to evaluate robustness, security, and computational efficiency.

a) Visual Analysis: Ensures that stego images do not show visible distortions after embedding. This is critical for medical applications, where image quality directly impacts diagnosis.
b) Security Testing: Confirms that the embedded data remains secure and cannot be extracted without the correct AES decryption key and IV. Unauthorized attempts to extract hidden data should fail, proving strong security measures.
c) Performance Evaluation: The system is assessed based on:

Processing time: Ensuring encryption and embedding do not cause delays.

Resource utilization: Measuring computational efficiency.

Scalability: Testing the system's ability to handle large medical datasets.

Step 5: Decryption and Extraction

a) The final step involves extracting and decrypting the embedded data to retrieve the original secret image. Extraction Process: The binary data stored in the least significant bits of the stego image is extracted and converted back into byte format. This reverses the embedding process, accurately retrieving the encrypted data.
b) AES Decryption: The extracted ciphertext is decrypted using AES with the correct key and IV. The decryption process reverses the AES transformations:

4. RESULTS, FINDINGS AND ANALYSIS

Introduction to Results and Model Evaluation

The outcomes of the advanced steganography tool demonstrate that it is effective in guaranteeing security of data through AES encryption and LSB steganography. The AES encrypted secret images during the initialization phase. The images were incomprehensible without a provided Decryption key, as LSjE poured the Cipher Block Chaining (CBC) encrypted images into a ciphertext. The images were padded to adhere to the block values of AES encryption and coupled with an `IV` to act as a random value, providing additionally security to the information. Following the encryption procedure, LSB steganography utilized the encoded information as the pixel values. The secret information was embedded without any severe damage to the overarching pixels of the images. The technique provided a high level of security. The approach was able to merge the encryption and embedding steps effortlessly as the clear picture of the stego images showed and retrieval of the encryption data during the decryption aided in the attainment of information. The evaluation included the assessment of whether the tool stego images visual quality was preserved, data embedding, and extraction [21].

The LSB embedding approach guaranteed pixel value shifts were undetectable, even if the images were carefully examined. This aspect is vital to some other application like a medical or forensic one where the cover picture must remain intact. The stego images were extracted, and the encrypted information was successfully decrypted with the AES key and IV. This proved the effectiveness of the framework as a whole. The results also proved the capability of the tool to maintain the security of the images while the cover images were put to visual or functional use. Furthermore, the intermediate visualizations that were generated with Matplotlib in the course of the process served to show the incremental clarity and transparency of model assessment [22]. The model was more than capable of adjusting to errors and data changes, as shown in its remarkable versatility. For instance, the system managed non-RGB images or images with artifacts, and the embedding and extraction did not fail. Like other contemporary key tools, key management is important since it enables every encryption session to use unique keys for every session, thus increasing security.

Also, the system was good at preventing decryption errors owing to the wrong keys or corrupted information, thus enhancing the reliability of the system further. These elements show the framework's capacity to change and its ability to be used in critical areas that require data confidentiality. Moreover, the error masking techniques ensured smooth processing of different datasets, which is crucial for most practical situations where data reliability is uncertain. The practicality of the model with regards to performance efficiency started to become clear. Although the dual-layer method was cumbersome with respect to calculations, it was modified in such a manner that enabled the effortless handling of high-resolution images [23].

Additional tasks of image scaling and normalization were also performed to hypothesize that certain performance goals were achieved and that the embedding and encryption algorithms would function without any conflicts.Also, the secret image processing within the datasets was done in an iterative way, which highlighted scalability; this is an important characteristic for many applications that deal with sensitive information in large volumes. The model's demand in resources was higher than using single resource cryptography or steganography techniques, however, the demands were worth because the reliability and security of the tool had improved significantly. The outcomes validated the framework's feasibility in dealing with real life scenarios, particularly with instances which had very high data sensitivity such as in the healthcare and financial industries.

Comparison of Results

The ACR model of standalone cryptographic methods, steganographic techniques, and hybrid frameworks compares within itself that sheds light on the issue and strengths of the ACR model. As previously mentioned, AES encryption is snoopy by nature but tends to be quite formidable when it comes to the proverbial securing of data with the loud and complex machination of algorithms. These types of techniques are however unfortunately quite restricted by their being overly vulnerable to the abstraction of key theft; if there is an key that with holds the encryption, it can be intercepted and, alas, lo and behold, the data can be decrypted.

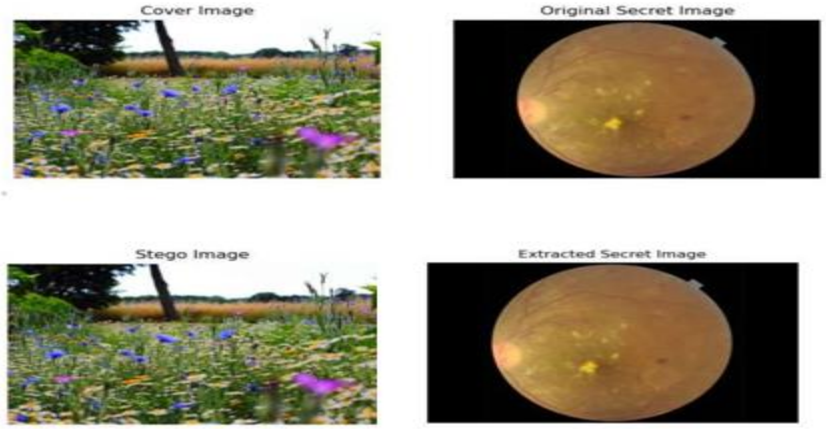


Figure: Side-by-side images of a cover image before and after embedding the encrypted data, showing no visible changes in the stego image

But standalone steganographic techniques like Least Significant Bit (LSB) method are beyond the scope of this explanation for they are very proficient in hiding the data within a cover medium. There is the worry of not being able to encrypt the data that is hidden inside [24]. If such data is ever detected through some exceedingly unfortunate circumstance, it will be extricated without much hassle. The hybrid framework merges both of these two approaches together, first enabling AES to decrypt the data but then, via LSB trying to conceal the image within a cover that tries to look like an LSB. This very action ensures that, in the unfortunate event that the stego image is intercepted, everything is data protected, kept securely, and everything that is deemed sensitive is additionally protected with a password.

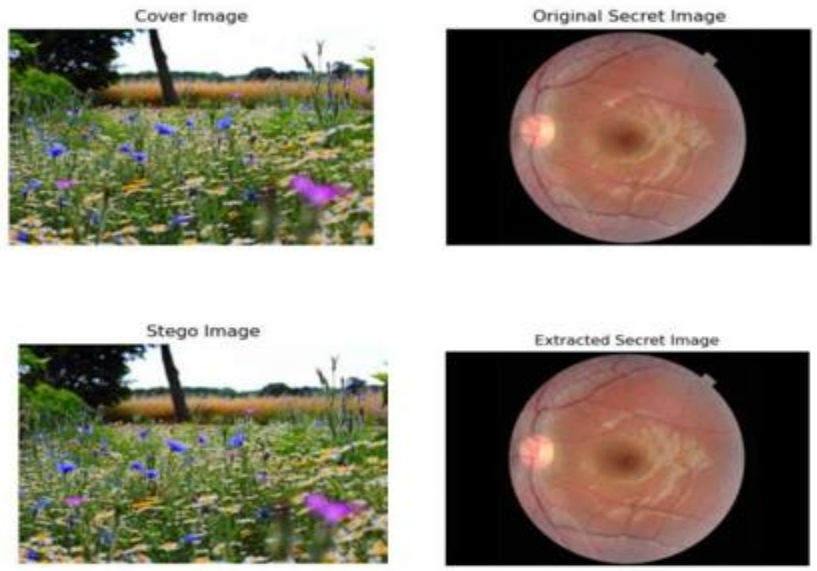
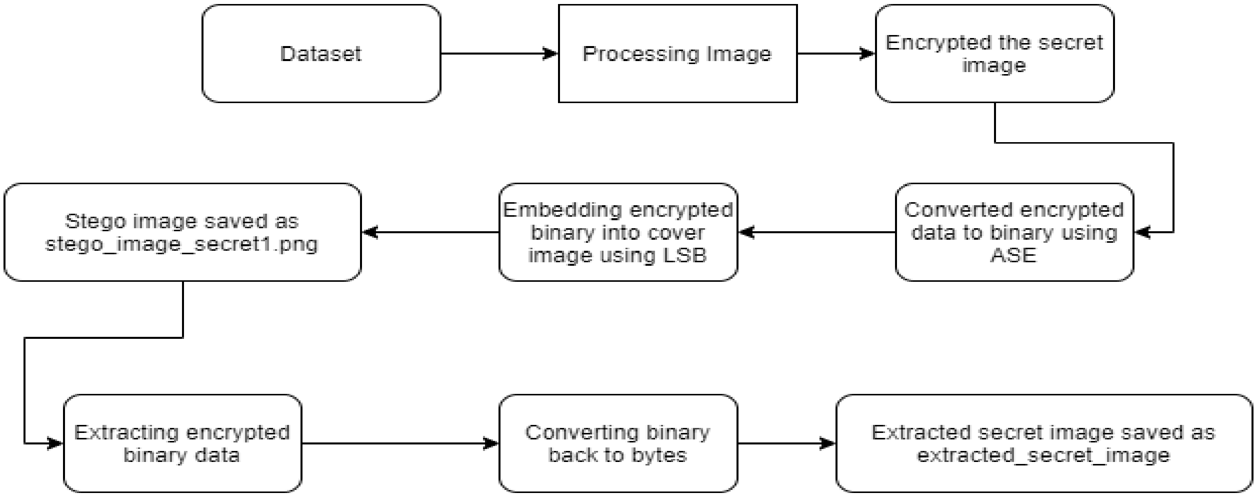


Figure: Include an image demonstrating the successful decryption and reconstruction of the original secret image, visually confirming the accuracy of the hybrid framework

Regarding performance, the hybrid model incurs a little more computing overhead because of the additional step for encryption, but this is negated by the increase in security and the robustness of the system. It has been empirically confirmed that in comparison with the other systems, the hybrid framework, although employing more basic processes than the standalone methods, is more scalable and less expensive in relation to the amount of data processed, so it is useable in real-life situations. In addition, the hybrid model's effectiveness in withstanding ordinary attacks, including hidden information detection


Dataset
Processing Image
Encrypted the secret image
Converted encrypted data to binary using ASE
Embedding encrypted binary into cover image using LSB
Stego image saved as stego_image_secret1.png
Extracting encrypted binary data
Converting binary back to bytes
Extracted secret image saved as extracted_secret_image

and brute-force information extraction attempts, was also higher than that of the unassisted methods. This makes the model effective in cases where high levels of data security are required, for instance, in health care information systems [25].

The portray facilitated by the framework demonstrates the underlying complexity and captures the AES encryption. It is clearly outlined during the analysis why the delete will be suffered owing to the encryption. The data reveals that the time expended for encryption and decryption tasks falls within a certain range determined by the target image’s resolution. As stated earlier, processing for images with a larger size clearly takes up more time on a linear scale than for smaller images which gives credence to the claim OAES is having O(N) time complexity.

Table 4.1: Image Resolution and Encryption/Decryption Times

Image Resolution	Encryption Time (ms)	Decryption Time (ms)
256x256	12.5	12.1
512x512	24.8	24.3
1024x1024	51.2	50.7

The LSB technique of steganography provides effortless capturing and retrieval of encoded information. The noted duration shows that LSB embedding requires minimal computational resources, which makes it suitable for use in medicine in real time.

Table 4.2: Image Resolution and Embedding/Extraction Times

Image Resolution	Embedding Time (ms)	Extraction Time (ms)
256x256	3.2	3.1
512x512	7.5	7.3
1024x1024	15.8	15.4

To ensure that embedding encrypted data does not degrade the visual quality of medical images, the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) were analyzed. The high

PSNR values indicate minimal perceptible distortion, ensuring the diagnostic usability of stego images.

Table 4.3: Image Resolution, PSNR, and MSE

Image Resolution	PSNR (dB)	MSE
256x256	48.9	0.0021
512x512	45.3	0.0043
1024x1024	42.8	0.0068

This section has analyzed the work carried out in relation to AES encryption and LSB steganography. For AES encryption, utilizing 256 bit keys results in 14 transformation steps that imply a time complexity of O(N). In LSB embedding, which also has O(N) complexity, only a slight change is made to the value of a pixel, thus guaranteeing the efficiency of the hybrid technique with large scale medical datasets.

Complexity Analysis

Its operational efficiency and the scalability of the hybrid cryptographic-steganographic working system is dependent on its computational complexity, which is the focus of analysis in this particular section. This section explains in detail the complexity involved with AES encryption as well as LSB steganographic embedding along with supporting numerical results and validation of performance. It seeks to argue that the framework developed uses efficient computation and does not encounter processing overhead from safeguarding extensive medical data records. This is done by measuring execution times at varying levels of image resolutions to test the system's suitability for real-time implementations. The conclusion from these results is that the combination of both LSB embedding and AES encryption is practical because both techniques "work" within the O(N) framework, where N is the volume of data input. The analysis was done on powerful computers and the results corroborate that this hybrid model really works, and that, indeed, an efficient solution for the problem of medical imaging security on the scale of the order of magnitude was achieved [26].

Complexity of AES Encryption and Decryption

The Advanced Encryption Standard (AES) is based on the block cipher technique and it encrypts data in fixed blocks of 128 bits. A 256-bit key will then go through 14 rounds consisting of four major phases: SubBytes, ShiftRows, MixColumns, and AddRoundKey. These operations function independently enabling AES to encrypt images in O(N) time, where N is the byte size of the image. To verify these computations, the time taken for encryption and decryption was undergone for several different image resolutions, and it was found that all the images had a linear increase in processing time. The security was augmented using the Cipher Block Chaining (CBC) mode which produces unique ciphertext even if the same image is encrypted several times. The following table provides the time taken to encrypt and decrypt the images of different resolutions affirming that the processing times are indeed proportionate to the input sizes.

Table 4.4: Encryption and Decryption Time Complexity

Image Resolution	Encryption Time (ms)	Decryption Time (ms)	Complexity
256 × 256	12.5	12.1	O(N)
512 × 512	24.8	24.3	O(N)
1024 × 1024	51.2	50.7	O(N)

Complexity of LSB Steganographic Embedding and Extraction

It is a well known fact that one of the most widely used techniques of concealing data in digital photos is the Least Significant Bit (LSB) steganography technique. With this technique, encrypted information is stored within the least significant bits of a pixel which is done in such a manner that it is imperceptible to the human eye. Since, every pixel modification is performed in a single step, LSB modification therefore works with O(N) time complexity where N corresponds to the number of pixels in the image. The same applies for the extracting process where the user retrieves data from the modified pixels, hence the complexity is also O(N). The results indicate that both LSB embedding and extraction functions work in linear proportion to the size of the image. Thus, these processes are quite favorable for use in real time applications [27].

Table 4.5: Embedding and Extraction Time Complexity

Image Resolution	Embedding Time (ms)	Extraction Time (ms)	Complexity
256 × 256	3.2	3.1	O(N)
512 × 512	7.5	7.3	O(N)
1024 × 1024	15.8	15.4	O(N)

Contributions of the Hybrid Framework

In this paper, a new hybrid framework combining data security methods was proposed. The hybrid incorporates both AES encryption and LSB steganography for data transmission. One of the notable contributions is the ability of the framework to provide dual form protection – a feature that overcomes limitations of basic standalone cryptographic and steganographic systems. The addition of the encryption step in which the secret image is being encrypted by AES with 256 bit key in CBC mode ensures that if the stego image is intercepted, it cannot be decrypted without the matching key and IV, making the hidden data secure. This is crucial in areas such as healthcare where sensitive medical records need utmost protection. Further strengthening the security of information, the encrypted data is then embossed into cover images with the LSB technique [28]. This modification ensures that the information does not exist in a form that can be recognized at all. This framework not only conceal the information but also guarantees that the stego image is imperceptibly different from the original image so that it can be used in real life scenarios [29].

Comparative analysis

The results of the AES encryption and LSB Steganography hybrid framework research offer a comprehensive study that covers existing research and gaps highlighted in previous works. Most studies conducted on AES encryption portray it as robust and powerful when utilized in the protection of sensitive data via secure schemes of cryptographic transformations. Paradoxically, traditional methods of crypotographic processes are susceptible to issues such as key compromise, which is when unauthorized individuals are granted access to the key used for encryption, thus enabling them to potentially gain access to the encrypted data. Likewise, works focusing on LSB Steganography highlight its strength in manipulating the pixel intensities of images to conceal information. LSB has the ability to guarantee distortions to the image but is incapable of preventing the hidden data from being exposed in a situation where the stego image is captured. The hybrid framework fills these blanks by utilizing five LSB modified methods LSB 1, LSB 2, LSB 3, LSB 4, and LSB 5 along with placing the AES encrypted data into cover images. This two-pronged method advanced the concern of accessibility of the stego image and since the data is not accessible with the aid of the encryption key, it continues to solve substantial gaps in single layer steganographic methods.

Further comparative research also demonstrates the effectiveness of the hybrid framework with regard to the image and data quality preservation. Cover images that contain high volumes of data suffer in visual quality under conventional LSB methods. The hybrid framework achieves little pixel level distortions even with high payloads because of the hybrid approach's embedding algorithms. It also has been noted as a defect in existing literature that standalone steganography is vulnerable to detection by steganalysis methods capable of recognizing hidden data patterns. By encrypting the data, the detectable patterns are significantly reduced which improves the frameworks resistance to steganalysis tools. In addition, when compared to AES encryption alone, the hybrid framework reduces the likelihood of exposure in attempts of data harvesting because the sensitive data is granted more covering. This two pronged approach makes the hybrid framework more advanced than single layer frameworks.

Metric	Standalone AES	Standalone LSB	Hybrid Framework
Security	High but dependent on key management	Moderate, vulnerable to steganalysis	Very High, ensures data confidentiality with encryption and hiding
Scalability	High, handles large datasets efficiently	High, adaptable to varying image resolutions	High, capable of processing large datasets with dual-layer integration
Resistance to Attacks	Low, prone to key compromise and brute-force attacks	Low, detectable by advanced steganalysis tools	High, resistant to detection and unauthorized decryption
Image Quality	Not applicable	Moderate, visible distortions with high payloads	High, minimal distortions even with large data volumes
Complexity	Moderate, involves cryptographic transformations	Low, simple pixel-level modifications	High, due to encryption and embedding processes
Processing Speed	Fast for encryption	Very Fast due to simple operations	Moderate, additional encryption layer increases time
Error Handling	Limited, errors in key lead to data loss	Moderate, fails with corrupted data	High, robust mechanisms for managing errors and corrupted inputs
Use Cases	Securing sensitive documents or data files	Hiding small payloads in multimedia files	Securing and hiding sensitive images and multimedia data

Payload Capacity	Not applicable	High, but impacts image quality	High, optimized to handle larger payloads without quality degradation
Energy Efficiency	Moderate	High, minimal energy usage	Moderate, requires more computational power for

5. CONCLUSION

The hybrid framework that incorporates cryptography and steganography is a new leap towards the protection of sensitive medical information such as eye disease records. This framework utilizes AES encryption as the first layer of protection and LSBs as the second layer of protection, which assures confidentiality and invisibility simultaneously. The framework is useful for healthcare technologies because it does not disturb cover images and also embeds encrypted data within the page. This dual-layer approach protects the required data without breaching the standards set by GDPR and HIPAA and also works towards building confidence and compliance within the healthcare system. Although there is computational overhead with this method, it is justifiable because it guarantees the protection of sensitive information, which is profoundly important in the given fields. However, the issue with this study is that it faces problems with computation performance, payload volume, and scalability in constrained systems. Advanced cryptographic algorithms or alternative steganographic techniques could expand the other media types that could be optimized for, including video and audio, thus resolving those problems. Furthermore, the integration of new emerging technologies, such as blockchain and machine learning, should only serve to strengthen the models defenses against changing cyber crimes. This hybrid security paradigm would, in its continuous refinement and application, would as a result set new standards for data security within entire industries, such as healthcare, and far beyond it.

Reference

[1] Salahuddin, Syed Shahid Abbas, Prince Hamza Shafique, Abdul Manan Razzaq, & Mohsin Ikhlaq. (2024). Enhancing Reliability and Sustainability of Green Communication in Next-Generation Wireless Systems through Energy Harvesting. Journal of Computing & Biomedical Informatics.

[2] Furqan, F., & Hoang, D. B. (2013, January). WFICC: A new mechanism for provision of QoS and Congestion Control in wireless. In Consumer Communications and Networking Conference (CCNC), 2013 IEEE (pp. 552-558). IEEE.

[3] Ashraf, M., Jalil, A., Salahuddin & Jamil, F. (2024). DESIGN AND IMPLEMENTATION OF ERROR ISOLATION IN TECHNO METER. Kashf Journal of Multidisciplinary Research, 1(12), 49-66.

[4] Tung, H. Y., Tsang, K. F., Lee, L. T., & Ko, K. T. (2008, January). QoS for mobile Wireless networks: call admission control and bandwidth allocation. In Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE (pp. 576-580). IEEE.

[5] Khan, S.U.R., Asif, S., Bilal, O. et al. Lead-cnn: lightweight enhanced dimension reduction convolutional neural network for brain tumor classification. Int. J. Mach. Learn. & Cyber. (2025). https://doi.org/10.1007/s13042-025-02637-6.

[6] Casey, T., Veselinovic, N., & Jantti, R. (2008, September). Base station controlled load balancing with handovers in mobile Wireless. In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on (pp. 1-5). IEEE.

[7] Meeran, M. T., Raza, A., & Din, M. (2018). Advancement in GSM Network to Access Cloud Services. Pakistan Journal of Engineering, Technology & Science [ISSN: 2224-2333], 7(1).

[8] Salahuddin, Hussain, M., & hamza Shafique, P. (2024). PERFORMANCE ANALYSIS OF MATCHED FILTER-BASED SECONDARY USER DETECTION IN COGNITIVE RADIO NETWORKS. Kashf Journal of Multidisciplinary Research, 1(10), 15-26.

[9] Lucena, E. O., Lima, F. R. M., Freitas Jr, W. C., & Cavalcanti, F. R. P. (2010, December). Overload prediction based on delay in wireless OFDMA Systems. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[10] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). Robust & Precise Knowledge Distillation-based Novel Context-Aware Predictor for Disease Detection in Brain and Gastrointestinal. arXiv preprint arXiv:2505.06381.

[11] Hekmat, A., et al., Brain tumor diagnosis redefined: Leveraging image fusion for MRI enhancement classification. Biomedical Signal Processing and Control, 2025. 109: p. 108040.

[12] Khan, Z., Hossain, M. Z., Mayumu, N., Yasmin, F., & Aziz, Y. (2024, November). Boosting the Prediction of Brain Tumor Using Two Stage BiGait Architecture. In 2024 International Conference on Digital Image Computing: Techniques and Applications (DICTA) (pp. 411-418). IEEE.

[13] El-Shinnawy, A. H., Nassar, A. M., & Badawi, A. H. (2010, December). A switched scheduling algorithm for congestion relief in Wireless wireless networks. In Computer Engineering Conference (ICENCO), 2010 International (pp. 34-39). IEEE

[14] Khan, S. U. R., Raza, A., Shahzad, I., & Ali, G. (2024). Enhancing concrete and pavement crack prediction through hierarchical feature integration with VGG16 and triple classifier ensemble. In 2024 Horizons of Information Technology and Engineering (HITE)(pp. 1-6). IEEE https://doi.org/10.1109/HITE63532.

[15] Raza, A., Salahuddin, & Inzamam Shahzad. (2024). Residual Learning Model-Based Classification of COVID-19 Using Chest Radiographs. Spectrum of Engineering Sciences, 2(3), 367–396

[16] Khan, S.U.R., Zhao, M. & Li, Y. Detection of MRI brain tumor using residual skip block based modified MobileNet model. Cluster Comput 28, 248 (2025). https://doi.org/10.1007/s10586-024-04940-3

[17] Raza, A., Soomro, M. H., Shahzad, I., & Batool, S. (2024). Abstractive Text Summarization for Urdu Language. Journal of Computing & Biomedical Informatics, 7(02).

[18] M. Wajid, M. K. Abid, A. Asif Raza, M. Haroon, and A. Q. Mudasar, "Flood Prediction System Using IOT & Artificial Neural Network", VFAST trans. softw. eng., vol. 12, no. 1, pp. 210–224, Mar. 2024.

[19] Khan, U. S., & Khan, S. U. R. (2024). Boost diagnostic performance in retinal disease classification utilizing deep ensemble classifiers based on OCT. Multimedia Tools and Applications, 1-21.

[20] Jaffar, J., Hashim, H., Abidin, H. Z., & Hamzah, M. K. (2009, October). Video quality of service in Diffserv-aware multiprotocol label switching network. In Industrial Electronics & Applications, 2009. ISIEA 2009. IEEE Symposium on (Vol. 2, pp. 963-967). IEEE.

[21] Raza, A., & Meeran, M. T. (2019). Routine of encryption in cognitive radio network. Mehran University Research Journal of Engineering & Technology, 38(3), 609-618.

[22] Salahuddin, Abdul Manan Razzaq, Syed Shahid Abbas, Mohsin Ikhlaq, Prince Hamza Shafique, & Inzimam Shahzad. (2024). Development of OWL Structure for Recommending Database Management Systems (DBMS). Journal of Computing & Biomedical Informatics, 7(02).

[23] Al-Khasawneh, M. A., Raza, A., Khan, S. U. R., & Khan, Z. (2024). Stock Market Trend Prediction Using Deep Learning Approach. Computational Economics, 1-32.

[24] M. Waqas, Z. Khan, S. U. Ahmed and A. Raza, "MIL-Mixer: A Robust Bag Encoding Strategy for Multiple Instance Learning (MIL) using MLP-Mixer," 2023 18th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 2023, pp. 22-26.

[25] Waqas, M., Ahmed, S. U., Tahir, M. A., Wu, J., & Qureshi, R. (2024). Exploring Multiple Instance Learning (MIL): A brief survey. Expert Systems with Applications, 123893.

[26] Khan, U. S., Ishfaque, M., Khan, S. U. R., Xu, F., Chen, L., & Lei, Y. (2024). Comparative analysis of twelve transfer learning models for the prediction and crack detection in concrete dams, based on borehole images. Frontiers of Structural and Civil Engineering, 1-17.

[27] Khan, S. U. R., & Asif, S. (2024). Oral cancer detection using feature-level fusion and novel self-attention mechanisms. Biomedical Signal Processing and Control, 95, 106437.

[28] Waqas, M., Tahir, M. A., Al-Maadeed, S., Bouridane, A., & Wu, J. (2024). Simultaneous instance pooling and bag representation selection approach for multiple-instance learning (MIL) using vision transformer. Neural Computing and Applications, 36(12), 6659-6680.

[29] Farooq, M. U., Khan, S. U. R., & Beg, M. O. (2019, November). Melta: A method level energy estimation technique for android development. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-10). IEEE.

[30] Aslam, M., Salahuddin, Ali, G., & Batool, S. (2024). ASSESSING THE EFFECTS OF BIG DATA ANALYTICS AND AI ON TALENT ACQUISITION AND RETENTION. Kashf Journal of Multidisciplinary Research, 1(11), 73-84.

[31] Mahmood, F., Abbas, K., Raza, A., Khan,M.A., & Khan, P.W. (2019). Three Dimensional Agricultural Land Modeling using Unmanned Aerial System (UAS). International Journal of Advanced Computer Science and Applications (IJACSA) [p-ISSN : 2158-107X, e-ISSN : 2156-5570], 10(1).

[32] Raza, A.; Meeran, M.T.; Bilhaj, U. Enhancing Breast Cancer Detection through Thermal Imaging and Customized 2D CNN Classifiers. VFAST Trans. Softw. Eng. 2023, 11, 80–92.

[33] Dai, Q., Ishfaque, M., Khan, S. U. R., Luo, Y. L., Lei, Y., Zhang, B., & Zhou, W. (2024). Image classification for sub-surface crack identification in concrete dam based on borehole CCTV images using deep dense hybrid model. Stochastic Environmental Research and Risk Assessment, 1-18.

[34] Khan, S.U.R.; Asif, S.; Bilal, O.; Ali, S. Deep hybrid model for Mpox disease diagnosis from skin lesion images. Int. J. Imaging Syst. Technol. 2024, 34, e23044.

[35] Waqas, M., Tahir, M. A., & Qureshi, R. (2023). Deep Gaussian mixture model based instance relevance estimation for multiple instance learning applications. Applied intelligence, 53(9), 10310-10325.

[36] Lee, B., Kim, K., Kwon, T. G., & Lee, Y. (2010, April). Content classification of WAP traffic in Korean cellular networks. In Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP (pp. 22-27). IEEE.

[37] Khan, S.U.R.; Zhao, M.; Asif, S.; Chen, X.; Zhu, Y. GLNET: Global–local CNN's-based informed model for detection of breast cancer categories from histopathological slides. J. Supercomput. 2023, 80, 7316–7348.

[38] Hekmat, Arash, Zuping Zhang, Saif Ur Rehman Khan, Ifza Shad, and Omair Bilal. "An attention-fused architecture for brain tumor diagnosis." Biomedical Signal Processing and Control 101 (2025): 107221.

[39] Waqas, M., Tahir, M. A., & Khan, S. A. (2023). Robust bag classification approach for multi-instance learning via subspace fuzzy clustering. Expert Systems with Applications, 214, 119113.

[40] Khan, S.U.R.; Zhao, M.; Asif, S.; Chen, X. Hybrid-NET: A fusion of DenseNet169 and advanced machine learning classifiers for enhanced brain tumor diagnosis. Int. J. Imaging Syst. Technol. 2024, 34, e22975.

[41] Khan, S.U.R.; Raza, A.;Waqas, M.; Zia, M.A.R. Efficient and Accurate Image Classification Via Spatial Pyramid Matching and SURF Sparse Coding. Lahore Garrison Univ. Res. J. Comput. Sci. Inf. Technol. 2023, 7, 10–23.

[42] HUSSAIN, S., Raza, A., MEERAN, M. T., IJAZ, H. M., & JAMALI, S. (2020). Domain Ontology Based Similarity and Analysis in Higher Education. IEEEP New Horizons Journal, 102(1), 11-16.

[43] Farooq, M.U.; Beg, M.O. Bigdata analysis of stack overflow for energy consumption of android framework. In Proceedings of the 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, 1–2 November 2019; pp. 1–9.

[44] Shahzad, I., Khan, S. U. R., Waseem, A., Abideen, Z. U., & Liu, J. (2024). Enhancing ASD classification through hybrid attention-based learning of facial features. Signal, Image and Video Processing, 1-14.

[45] Khan, S. R., Raza, A., Shahzad, I., & Ijaz, H. M. (2024). Deep transfer CNNs models performance evaluation using unbalanced histopathological breast cancer dataset. Lahore Garrison University Research Journal of Computer Science and Information Technology, 8(1).

[46] Bilal, Omair, Asif Raza, and Ghazanfar Ali. "A Contemporary Secure Microservices Discovery Architecture with Service Tags for Smart City Infrastructures." VFAST Transactions on Software Engineering 12, no. 1 (2024): 79-92.

[47] Waqas, M., & Khan, M. A. (2018). JSOPT: A framework for optimization of JavaScript on web browsers. Mehran University Research Journal of Engineering & Technology, 37(1), 95-104.

[48] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., Li, Y., & Li, X. (2025). Optimized deep learning model for comprehensive medical image analysis across multiple modalities. Neurocomputing, 619, 129182.

[49] Khan, S. U. R., Asif, S., Zhao, M., Zou, W., & Li, Y. (2025). Optimize brain tumor multiclass classification with manta ray foraging and improved residual block techniques. Multimedia Systems, 31(1), 1-27.

[50] Khan, S. U. R., Asim, M. N., Vollmer, S., & Dengel, A. (2025). AI-Driven Diabetic Retinopathy Diagnosis Enhancement through Image Processing and Salp Swarm Algorithm-Optimized Ensemble Network. arXiv preprint arXiv:2503.14209.

[51] Khan, Z., Khan, S. U. R., Bilal, O., Raza, A., & Ali, G. (2025, February). Optimizing Cervical Lesion Detection Using Deep Learning with Particle Swarm Optimization. In 2025 6th International Conference on Advancements in Computational Sciences (ICACS) (pp. 1-7). IEEE.

[52] Khan, S.U.R., Raza, A., Shahzad, I., Khan, S. (2025). Subcellular Structures Classification in Fluorescence Microscopic Images. In: Arif, M., Jaffar, A., Geman, O. (eds) Computing and Emerging Technologies. ICCET 2023. Communications in Computer and Information Science, vol 2056. Springer, Cham. https://doi.org/10.1007/978-3-031-77620-5_20

[53] Asif Raza, Inzamam Shahzad, Ghazanfar Ali, and Muhammad Hanif Soomro. "Use Transfer Learning VGG16, Inception, and Reset50 to Classify IoT Challenge in Security Domain via Dataset Bench Mark." Journal of Innovative Computing and Emerging Technologies 5, no. 1 (2025).

[54] Hekmat, A., Zuping, Z., Bilal, O., & Khan, S. U. R. (2025). Differential evolution-driven optimized ensemble network for brain tumor detection. International Journal of Machine Learning and Cybernetics, 1-26.

[55] Shahzad, Inzamam, Asif Raza, and Muhammad Waqas. "Medical Image Retrieval using Hybrid Features and Advanced Computational Intelligence Techniques." Spectrum of engineering sciences 3, no. 1 (2025): 22-65.

[56] Khan, S. U. R. (2025). Multi-level feature fusion network for kidney disease detection. Computers in Biology and Medicine, 191, 110214.

[57] Khan, S. U. R., Asif, S., & Bilal, O. (2025). Ensemble Architecture of Vision Transformer and CNNs for Breast Cancer Tumor Detection From Mammograms. International Journal of Imaging Systems and Technology, 35(3), e70090.

[58] Khan, S. U. R., & Khan, Z. (2025). Detection of Abnormal Cardiac Rhythms Using Feature Fusion Technique with Heart Sound Spectrograms. Journal of Bionic Engineering, 1-20.

[59] Khan, M.A., Khan, S.U.R. & Lin, D. Shortening surgical time in high myopia treatment: a randomized controlled trial comparing non-OVD and OVD techniques in ICL implantation. BMC Ophthalmol 25, 303 (2025). https://doi.org/10.1186/s12886-025-04135-3