Multimedia Tools and Applications (2021) 80:21165–21202
https://doi.org/10.1007/s11042-021-10723-4

Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems

R. Denis[1] · P. Madhubala[2]

Received: 18 February 2020 / Revised: 4 February 2021 / Accepted: 10 February 2021 /
Published online: 13 March 2021

Abstract

The exponential rise in the development of cloud computing environments in the healthcare field, the protection and confidentiality of the medical records become a primary concern for healthcare services applications. Today, health data stored in the cloud is highly confidential information concealed to avoid unauthorized access to protect the patient's information. As cloud-based medical data transmission becomes more common, it receives growing attention from researchers and academics. Despite the potential for misuse, medical data transmitted through unreliable networks can be manipulated or compromised. The current cryptosystems alone are not sufficient to deal with these issues, and hence this paper introduces a new hybridization of data encryption model to shelter the diagnosis data in medical images. The proposed model is developed by combining either 2D Discrete Wavelet Transform 1 Level (2D-DWT-1 L) or 2D Discrete Wavelet Transform 2 Level (2D-DWT-2 L) steganography with the proposed hybrid encryption scheme. The hybrid encryption scheme is built by strategically applying Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to secure diagnosis data to be embedded with the RGB channels of medical cover image. One of the key novelties is the use of an Adaptive Genetic Algorithm for Optimal Pixel Adjustment Process (AGA-OPAP) that enriches data hiding ability as well as imperceptibility features. To evaluate the efficiency of the proposed model, numerical tests are performed. The results show that the proposed algorithm is capable of safely transmitting medical data. Comparison of results is carried out concerning the datasets with the state-of-the-art algorithm. In terms of various statistical measures, the results showed the superiority of the proposed algorithm, such as peak signal to noise ratio (PSNR), correlation, structural content (SC), structure similarity (SSIM), entropy, histogram, NPCR, UACI and embedding capacity. The proposed model can also prevent attacks, such as steganalysis or RS attacks.

✉ R. Denis
denisatshc@gmail.com

Extended author information available on the last page of the article

Keywords Encryption · Decryption · Data hiding · Cloud environment · Health information exchange · Adaptive genetic algorithm · Steganalysis

1 Introduction

The high-paced technological revolution and subsequent computing strategies have led to a broad horizon providing a range of applications of which medical image communication is predominant. Biomedical image transmission became one of the imminent needs in the current health care system to ensure reliable, seamless and secured data transmission across uncertain channels. The Internet of Things (IoT) and cloud healthcare models have helped to launch a vast amount of healthcare data that is being distributed across the network. It is vital to ensure the confidentiality and security of the patient's diagnosis from an IoT and cloud ecosystem [21].

The arrival of new developments has increased the amount of multimedia information exchanged between individuals, which has sparked concern for preserving personal information privacy and security [44]. Besides, mammoth data storage growth has led to the invention of new storage technologies such as cloud [55], fog [65], edge [52], etc., which have played a pivotal role in each organization's IT infrastructure. However, irrespective of communication and storage systems, information security is still a concern. Confidentiality, authentication, integrity and non-repudiation play a fair role among the protection components in shaping the security algorithms used to secure the transmission of multimedia artefacts such as text, images, audio, video, etc. The incredible amount of internet-enabled communication systems has produced enormous data in real-time to meet various application requirements, such as social networking sites, the healthcare sector, e-commerce, scientific communities, financial sectors and other industrial requirements surveillance and security systems, etc. Social media and entertainment, surveillance footages, user multimedia data, and IoT services require security measures and policies to protect their data from unauthorized access. Undeniably, enterprise software has undergone tremendous growth in many sectors and government departments, producing and communicating vast data volumes (including multimedia data). In reality, these data are used to make appropriate decisions and recommendations. The combination of multiple data sources and associated voluminous aggregation of data has given rise to the cloud computing paradigm.

One of the main advantages of cloud computing is that it allows data access by multiple stakeholders, real-time computation and decision-making using cloud resources regardless of location or geographical boundaries. However, until a robust protection measure is not provided, data exchange from one node or user to another or across the cloud platform is highly vulnerable. Security or seamless information sharing of private data, particularly multimedia data (video, audio, image) [21, 44, 55, 65], is critical concerns in the cloud computing world. In addition to secure communication, enabling computational efficiency is also critical, as it demands time-efficient and reliable computation to meet the application's real-time needs. This means ensuring the security, scalability and manageability of up-surging computational and allied communication requirements in the cloud computing world. Facilitating the privacy of digital information has now become unavoidable for the cloud setting, such as social media, healthcare, etc. [2, 24, 39, 40, 48, 55, 65, 66].

Medical data, including individual reports, clinical results, etc., are exchanged between hospitals information to decrease tests' redundancy. The exchange of medical information accelerates the care of patients. The sharing of medical data is, thus, the demand of the current era. One of the key concerns is that medical officers use the internet (cloud) to share medical data, which is fast but at the same time, secure such information. Different attempts have been made to protect medical data transmission by implementing various protocols such as HTTPs, but the secure transmission of medical data is still an open issue. When a miscreant gets access to data or retrieves the data or related information during communication networks, it can be easily altered or misused for any targeted or intended goals. Numerous attempts have been made to prevent such occurrences in implementing security systems; however, significant efforts are either creating data access security models or infrastructure security or applying several data security features [31]. Researchers have developed security mechanisms for which the user needs to be authenticated before accessing the data (access-control), or the data itself is protected so as not to expose secret information inside the data to the unauthorized user intruder. In recent years, various attempts have been made to strengthen data protection in the cloud. However, ensuring that both security and computing performance has remained an open issue for academics and industry.

Encryption of data is the most common cryptographic technique. Here, the data is used to be inserted or concealed within the image so that the attacker will not retrieve the data while the approved person will be provided with a key called the encryption/decryption key to retrieve the data. In this case, it is not easy to find a practical encryption/decryption key mainly due to the combination of numbers used to produce exponential key ranges as the key length increases linearly. Therefore, it is considered as an NP-hard problem. Also, locating a particular key is a search problem. The identity key length of the encryption/decryption key increases exponentially, so simple search methods such as linear and binary searching would not be possible. Metaheuristic algorithms have been introduced to deal with this sort of situation. Metaheuristic algorithms are algorithms for search and optimization. These techniques have been successfully used to solve complex problems of optimization [53, 67].

Among the powerful multimedia data privacy techniques, steganography and cryptosystems have played a decisive role in practice, but these methods are limited due to the growing prevalence of parallel attacks. There has been widespread attention to the Hybrid Cryptography and Steganography (HCS) model design, where the dual-level of security makes or offers better data security. However, as an application-specific scenario, preserving safe and attack resilient multimedia (medical data) transmission requires enhanced steganography and the cryptosystem to achieve the above specified eventual target.

This paper focuses on improving steganography and cryptosystems by realizing multimedia (medical data) communication over cloud infrastructure that is becoming vulnerable these days due to increased attack efforts. The Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm are the two principal algorithms used in this work for data encryption [41]. AES is a symmetric cipher where the same key is used on both sides [59]. It is generated by a fixed message block size of 128 bits of plain text and keys of length 128, 192, or 256 bits. When sending longer messages, it must be split up into 128-bit chunks. Longer keys make the cipher more challenging to crack, but they also impose a longer encrypt and decrypt method. On the other hand, RSA is a public key algorithm commonly used in the business and private communication sectors [6]. It has the benefit of a variable key size ranging from (2–2048) bits.

The primary research in hiding data began with steganography, which refers to the science and art of hiding information inside an image. The advantage of steganography is that it can be used without the transmission being detected to send classified messages. The DWT has immense spatial localization, frequency distribution, and multi-resolution features consistent with the theory of forms in the human visual system. This paper implements both 1-level and 2-level of DWT steganography techniques that work on the frequency domain. It segmented the image into parts by high and low iteration. Edge information is stored in the high iteration portion, while the low iteration part is often split into high and low iteration parts.

Steganography aims to prevent anyone from knowing secret information and remove the suspicion of hidden information. The message is a secret text to be sent and camouflaged in the carrier to remain harder to detect. There are two main aspects of any steganography method, which are embedding capacity and imperceptibility. However, these two properties are confusing because it is challenging to increase capability while preserving a steganography system's imperceptibility. Besides, for the use of data transfer communication protocols, few concealing information methods can be unconventional, but its future is promising.

Once performing secret data encryption, an enhanced Adaptive Genetic Algorithm assisted LSB embedding model is developed that helps to embed secret text (i.e., cipher data) into the cover image optimally without increasing or affecting PSNR or visual characteristics such as entropy, histogram patterns etc. Because the inclusion of secret text might impact pixel arrangement and resulting entropy, PSNR, histogram patterns and other statistical features such as regular and singular coefficients of image blocks, AGA algorithm was applied to perform Optimal Pixel Adjustment (OPAP) during LSB embedding. The proposed method is evaluated under statistical attack assessment, and it has demonstrated high PSNR, low entropy, negligible perceptibility, and histogram deviations. Such novelties can help the proposed model avoid attacks like Steganalysis attack or RS attacks which are well known for exploiting statistical variations in multimedia data to detect secret or hidden information. The overall model is built with MATLAB2018a tool. The proposed security achieves enhanced or augmented security for medical data communication over the cloud environment.

The remaining parts of the manuscript presented are given as follows. The related works are provided in Section 2, preceded in Section 3 by the proposed model. Section 4 examines the results obtained and their respective inferences. In Section 5, the conclusion of the overall research is given.

2 Related works

This section presents some of the main works on multimedia and medical data privacy using steganography and various related technologies. In recent years, the importance of healthcare services has been realized globally and has emerged as one of the dominant research domains across academia industries. However, the preservation of optimum medical data privacy is a must to ensure smooth and flawless processes. Steganography, being one of the most efficient medical data security approaches, applied image transformation schemes to incorporate essential data into the cover image (i.e., medical image). In reality, the efficiency of reversible steganography techniques depends solely on image transformation effectiveness, data embedding and pixel adaptation to allow maximum imperceptibility.

Razzaq et al. [46] proposed a fusion of encryption, steganography and watermarking for digital image security. Authors [46] developed three key components: (a) the original image was encrypted using the sizeable secret key by rotating pixel bits the right using XOR operator; (b) for steganography, the encrypted image was altered through the least significant bits (LSBs) of the cover image and stego images were obtained; and (c) stego images were watermarked in time and frequency domain to ensure ownership. This approach showed promising results, but it does not deal with data redundancy (repeated transmission of the same data).

Bairagi et al. [9] suggested three coloured image steganography method where the 1st and 3rd method used red, green and blue channels to provide security. On the other side, green and blue colours were used in the 2nd method to implement protection during data transmission.

Anwar et al. [7] implemented a model to safeguard any images, specifically clinical images. It seeks to balance digitalized clinical data integrity, ensuring the accessibility of desired information and information integrity to ensure that people's authorities can use the data. The AES encryption model is used initially in the primary region. In this process, the ear print has been integrated, from which seven values are filtered from the ear picture as a function vector. The developed model improved the protection of clinical images by transmitting online images that have to be provided with more security to prevent access by third parties.

Jain et al. [20] provided a safe transfer of the patient's medical information inside the medical cover image using a decision tree to conceal details. Breadth-first searching (BFS) was implemented at the sender end, in steganography, for mapping hidden cipher blocks to carrier images for data insertion. The RSA decryption algorithm was applied at the received end to extract the patient's confidential medical information. A single approved recipient could therefore understand the plain text. This technique yielded excellent results, but was not ideal for large and exponentially increasing search spaces.

Authors [30] suggested a stable method for colour image steganography using grey-level modification and multi-level encryption (MLE). The secret key and secret data were encrypted using the MLE algorithm before mapping it to the cover images' grey level. A transposing function was then added to the cover image before the data was hidden.

Zaw and Phyo et al. [32] used both cryptographic and steganographic topographies to add security features. The Blowfish encryption algorithm was used to enforce encryption. The superiority of the blowfish encryption algorithm over single encryption was represented experimentally. This method was straightforward and dealt with databases on a small scale.

Sreekutty and Baiju et al. [57] suggested a verification system for medical data integrity to introduce medical image transformation security. It works in two stages: (a) protection; and (b) verification. The message is embedded within the image using the 2-stage Haar DWT frequency in the HH band during the protection process. On the other hand, the extraction algorithm was used in the verification stage to extract the secret message and check the message's integrity.

Bashir et al. [10] described a new image encryption technique based on integrating shifted image blocks and basic AES, where the shifted algorithm technique is used to divide the image into blocks. In each block, a set of pixels will be available, and the blocks are used to perform a "swapping" technique so that the content of the data will not be the same as the original image. After being shuffled, the image will be processed using the AES algorithm for encryption. By running numerous simulations and displaying histograms, the test demonstrated the proposed algorithm's effectiveness. The algorithm worked well but was not able to manage the exponential growth in the search space.

Khalil et al. [22] suggested a method for studying image degradation from manipulating frequency components in medical images. The plaintext was encrypted using RSA-based ciphers (i.e. RC4) before being inserted. The Discrete Fourier Transform (DFT) was applied to convert the cover image into the frequency domain by decomposing it into its sinusoidal (sine and cosine) fundamental components in different frequencies. The results show that the image's quality is significantly diminished when the data to be embedded close to the low-frequency bands, and the effect decreases in the upper-frequency bands.

Li, L. et al. [26] suggested a secret image sharing scheme for embedding secret image shares consistent with the IoT-Cloud system. The proposed system consists of two modules; a module for generating shadow images to generate secret shares based on Shamir's polynomial, and the main formulation module for incorporating secret image shares into the cover image based on a 24-ary notational system.

Sajjad, M. et al. [47] introduced an assisted domain-specific mobile-cloud system to outsource medical stego-images for selective encryption to the cloud. The visual saliency detection model was used to detect the region of interest (ROI) from the transmitted image. The directed-edge steganography method was used to embed the detected ROI into the cover image and create the stego image sent to the cloud for selective encryption.

Vipula et al. [62] combined steganography with the AES crypto-algorithm to conceal confidential data inside the multimedia cover files. Saleh et al. [49] used the modified AES algorithm to encrypt the hidden message that was then processed into the cover image for hiding. However, recently, Duluta et al. [12] have found that such classical encryption-based models have numerous limitations that can restrict their suitability for the era of cloud computing.

Panchal et al. [37] applied steganographic cryptosystems for efficient data communication. Authors initially performed encryption by applying the encryption key combined with Chirikov mapping for image encryption, which transformed the input image into a cipher image. Authors applied steganography in the subsequent process in order to mask the cipher image inside the cover image.

Leung et al. [25] recommended unequal security encoding by implementing several encryption methods to encrypt various media sections of different significance. Ahmed et al. [4] developed a model based on a user interface in which the sender could pick the appropriate cover and secret message that was processed using ECC-based encryption, followed by LSB embedding. The data was processed through various methods to arrive at the same goal. To achieve better performance, Hajduk et al. [17] suggested image steganography where the hidden message was encrypted and inserted within the cover image data using QR codes (Quick Response Codes).

Mukhedkar et al. [34] also applied various ciphers such as DES, 3DES, AES, and blowfish encryption algorithms to encrypt the hidden data before embedding into a cover image for efficient and stable multimedia transmission. Unlike traditional cryptosystems, McEliece's cryptosystem was used by Alam et al. [5] to encrypt or decrypt data to improve data protection across wireless networks. Depicting limitations of the classical cryptosystems, Kumar et al. [23] formulated an asymmetric key cryptography algorithm for secure colour 3D data communication. Because the better multimedia data analysis technique such as wavelet analysis can enhance the confidential data's imperceptibility over an uncertain channel, Gupta et al. [16] recommended using Discrete Wavelet Transform (DWT). Authors applied DWT to split input image into four sub-bands, followed by data hiding within the splits. After hiding the text information, the image was compressed before transmission. The authors [30, 35] implemented a new hidden communication method for data that used RSA and AES combined with steganography.

Liao et al. [27] introduced a steganographic medical JPEG image scheme based on stabilizing inter-block DCT coefficient dependencies. Balakrishnan et al. [43] proposed a unique image crypto method in the transform domain using blended chaotic maps and Haar Integer Wavelet Transform (HIWT). A hybrid encryption algorithm was projected based on deoxyribonucleic acid and several chaotic maps to encrypt DICOM colour images by Divya et al. [45].

Mansour et al. [29] suggested the Discrete Ripplet Transformation technique for data embedding in medical cover images to ensure seamless communication over an unsecured network. Usman et al. [60] applied Swapped Huffman tree encoding to provide multiple encryptions of medical data. Hashim et al. [18] proposed a new Bit Invert System (BIS) based steganography scheme using three random control parameters to secure medical data. Nithya et al. [11] developed an integrated security framework using DNA coding methods and image encryption to provide enhanced security. Harnal et al. [54] have proposed a dynamic cryptography algorithm based on end-to-end cryptography (E2EE) to maintain integrity and confidentiality in the environment of multimedia cloud computing.

Stoyanov et al. [58], using a nuclear spin generator method, proposed a medical image stego hiding technique and discussed the results based on histogram analysis and peak signal-to-noise ratio. A robust, quasi-quantum walk-based image steganography mechanism has been introduced by Baseem et al. [1] to support secure transmission on the cloud-based E-healthcare platform. Madhusudhan et al. [28] created a stable multimedia transmission mechanism involving binary bits and the Arnold map.

Emy et al. [50] invented a stable colour image transmission system using the compression-encryption model and dynamic key generator, and a highly efficient symmetric key distribution. Pandey et al. [38] have developed a secure medical data transfer framework based on a bit mask driven genetic algorithm.

Rajesh Kumar et al. [42] suggested a hidden image communication scheme that uses visual cryptography and tetrological tiling patterns. The original image is first broken up into 4 × 4 sub-blocks. The alternative rows and columns of sub-blocks are grouped into tetrolet and non-tetrolet blocks. The proposed scheme encodes the original image's tetrolet blocks into meaningful secret shares using the tetrominoes patterns. The non-tetrolet blocks are entirely replaced by zero. Finally, a new shadow image is obtained at regular intervals with different tetrolet patterns. A dynamic virtual cluster cloud encryption using the hybrid steganographic image authentication algorithm was suggested by Venkataraman et al. [61]. With the hybrid blowfish and genetic operator, this model performs expeditiously and ensures greater security. The proposed model of Puspha et al. [8] was presented by combining the 2D DWT method with the hybridization of Blowfish and Two fish encryption algorithms.

In image encryption and cryptography theory, literature shows that only a few have used metaheuristic algorithms. Bio-inspired algorithms and evolutionary algorithms have been successfully implemented in recent research to solve secure multimedia (medical) data transmission. Considering these factors, a Discrete Wavelet Transform, LSB embedding, Adaptive GA-based OPAP, AES and RSA-based hybrid encryption has been built in this research (dual-level biomedical image security). The discussion of the proposed model of steganography is given in the following sections.

3 Proposed model

This paper proposes a security model for healthcare to safeguard the transfer of medical data in cloud environments. Four continuous processes make up the proposed model:

(1) The secret data is encrypted using a proposed hybrid encryption scheme, combining AES and RSA algorithms.

(2) The encrypted data is being concealed in a cover image in the RGB channels using either 2D-DWT-1 L or 2D-DWT-2 L and AGA based Optimal Pixel Adjustment Process produces a stego-image.

(3) Extraction of embedded data
(4) To recover the original data, the data extracted is decrypted.

3.1 Secret data encryption

There are numerous cloud-assisted application environments in which different data, including multimedia and text, are transmitted under uncertain channel conditions. Some of the typical applications are telemedicine in the healthcare sector, social media, etc. Such applications can even have composite data as the amalgamation of text and image (for example, telemedicine both patients scanning medical reports and allied diagnosis details in text). In such cases, ensuring respective seamless transmission is of utmost significance. Towards this motive, the proposed model can be a viable solution. However, ensuring multi-level security can have augmented strength to alleviate any breach of security or unauthorized data access. Considering it as an impetus, a hybrid encryption model is designed at first. Here, the prime motive behind this is to increase the level of security by applying two different cryptosystems together, which, as a result, can avoid any easy attack on the data.

Consequently, it can achieve a higher level of security. In the proposed model, we have exploited the efficacy of two well-known cryptosystems RSA and AES to design the hybrid encryption scheme. The proposed cryptographic model embodies the strategic implementation of both RSA and AES, which has been used to encrypt input text data that is first converted into ciphertext embedded within the medical image.

The cryptographic model $\mathbb{C} = \{\mathsf{F}\eta, \mathsf{F}\eta^{-1}, C, S, T\}$ encompasses encryption and decryption processes. During the encryption process, at first, the secret text data (it can be the diagnosis details of a patient which is expected to be transmitted along with the medical imaging reports) is split into two distinct parts, T_{odd} and T_{Even}. Splitting the text data does not signify dividing content in two fractional parts, instead once converting entire text into binary form, the overall bit sequence is processed in such way that the odd-sequence value is assigned to T_{odd}, while bits at even place or sequence is allocated to the T_{Even}component. Thus, it converts overall input text data into two data-chunk or components T_{odd} and T_{Even}. We applied AES cryptosystem to encrypt T_{odd} and while RSA was used for T_{Even} encryption. Considering computational efficiency demands, we considered 64-bit RSA, while AES was applied as 256-bit. RSA with low bit-size has often been criticized for having inferior robustness; however, such a hypothesis can be applied merely with RSA as a standalone encryption algorithm. Its implementation with AES-256 can help to achieve a dual goal. First, the amalgamation of AES-RSA as a cryptographic algorithm can avoid easy attack probability (which can be possible with standalone encryption). Second, the consideration of low-bit size can avoid unwanted computation that eventually will make it robust to serve real-time applications. Additionally, AES-256 is six times faster and more efficient than classical triple-DES. Therefore, the inclusion of AES as a cryptographic method seems viable towards an influential encryption environment. On the other hand, the combination of RSA with low-bit size can help to make overall encryption more robust to avoid any attack. In other words, the strategic amalgamation of AES-256 and RSA-64 can confuse the attacker(s) to get real and exact information of the data being processed or communicated.

In the proposed encryption model, AES-256 has 14 rounds of computation, while 64-bit RSA was applied as single round itself, as it does not employ round-computation for confusion creation (to avoid side-channel attack). Noticeably, AES applies an encryption key or the round key s to encrypt the text data component T_{odd}, while RSA being public-key cryptography applies a secret public key m to encrypt the data T_{Even}. We used a private key x to perform decryption of the RSA encrypted data at the receiver. On the contrary, we performed standard decryption method for AES encrypted data. To be noted, AES decryption is the reverse of encryption, which is performed by executing inverse round transformations to retrieve original text data (from the encrypted data). Here, inverse round transformation method applies four essential functions,*AddRoundKey*,*InvMixColumns*, *InvShiftRows* and *InvSubBytes*, sequentially. Thus, the overall process is mathematically modelled as follows:

$$C = \left\{ E_{AES}, E_{RSA}, T_{odd}, T_{Even}, \widehat{T}_{odd}, \widehat{T}_{Even}, s, m, x \right\} \tag{1}$$

$$\widehat{T}_{odd} = \{ E_{AES}(T_{odd}, s) \} \tag{2}$$

$$\widehat{T}_{Even} = \{ E_{RSA}(T_{Even}, m) \} \tag{3}$$

Hybrid Encryption Algorithm for Secret Data Encryption is given as follows:

```
Input: Secret Text Input Data ($S_{Text}$)
Output: Cipher Text, Keys
Initiate the process
Step-1 Split the input text $S_{Text}$ into two components $S_{Text\_odd}$ and $S_{Text\_Even}$
Step-2 Generate AES keys[57]
Step-3 Encrypt $S_{Text\_odd}$ using AES-256 bit key size
    $Enc\_S_{Text\_odd} = AES - 256\ (S_{Text_{odd}}, s)$
Step-4 Generate RSA keys (Public key $m$ and private key $x$)
Step-5 Encrypt $S_{Text\_Even}$ using 64 bit-RSA
    $Enc\_S_{Text\_Even} = RSA - 64(S_{Text\_Even}, m)$
Step-6 Accumulate the encrypted cipher data $Cipher_{\ F\_Total}$ by using both $Enc\_S_{Text\_odd}$and $Enc\_S_{Text\_Even}$
Step-7 $Enc_{Key} = AES(x, s)$ #$x$-round key, #s-secret key
Step-8 Generate $Cipher_{\ Tx} = Concatinate(Cipher_{\ F\_Total}, Enc_{Key})$
Step-9 Return $Cipher_{\ Tx}$ and $s$
End
```

Once the text data has been encrypted, it has been processed for AGA-OPAP assisted LSB embedding.

3.2 Embedding procedure and AGA based OPAP

To embed the critical information within the medical image to be transmitted over cloud infrastructure, it is essential to decompose the input cover image and embed the cipher data optimally, while ensuring minimum entropy, histogram variations, or PSNR reductions. In this process, DWT with HAAR mother wavelet is applied. The model starts by separating each colour channel's intensity (Red, Green and Blue). In each colour channel, the process of decomposition is then carried out. The method is split into two elements, namely compression and embedding. This approach will ensure the security of the image data and enable rapid encryption and decryption processes. It can also decrease the potency of attacks from frequency analysis, make it longer for brute force attacks, and minimize the plaintext redundancy so that cryptanalytic attacks can be thwarted. The 2D-DWT-2 L is formulated as a sequential transformation process with a low pass and high pass filters towards the image's row (blocks). The key reason for considering 2D-DWT-2 L coefficients is that it can significantly provide a significant local feature set for text-embedding without impacting image quality.

Moreover, it can provide a more depth (feature) space for embedding. A cumulative solution with the proposed encryption can help strengthen attack-resiliency and confusion. Performing embedding with a single layer can cause higher-visibility perceptibility and impact image quality post-embedding. On the other hand, embedding with higher-level coefficient can be more effective at the cost of increased computation, which cannot be suitable for contemporary real-time application demands.

For optimal use of high and low pass filters, a pragmatic transformation is necessary. In Fig.1, the process followed in steganography using DWT is shown. We can see that Fig. 1 highlights the method of the elemental decomposition of the image in $C_j(n \times m)$ dimensions which will be applied to the RGB colour channels. Further, the image of each colour channels is divided into four groups of frequency bands, which are stated as high-high (HH), a high-low (HL), a low-high (LH), and a low-low (LL) frequency bands as shown in Fig. 2. The proposed model is designed to support visually imperceptible steganography to ensure maximum possible visual-imperceptibility that ensures seamless communication and assists quality-data transmission, which is a must for cloud communication.

To achieve it, the proposed model implements the steganographic scheme $\hat{S} = \{\{F\eta, F\eta^{-1}, C, S, T\}\}$ comprises of Least Significant Bit (LSB) embedding, AGA-OPAP assisted embedding optimization and extraction processes. The embedding process takes a cover (medical) image C and a secret text message $Cipher_{Tx}$ T as input and generates a

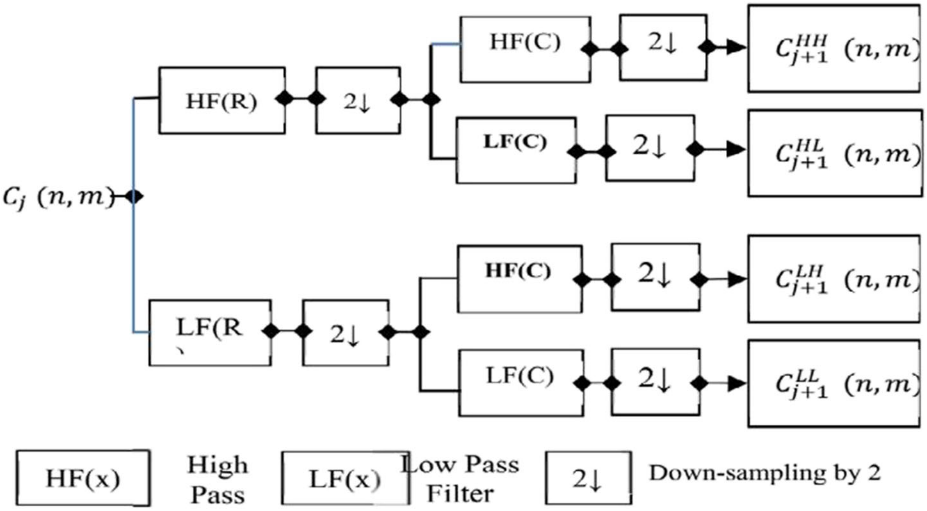


Fig. 1 2D-DWT-2 L decomposition process

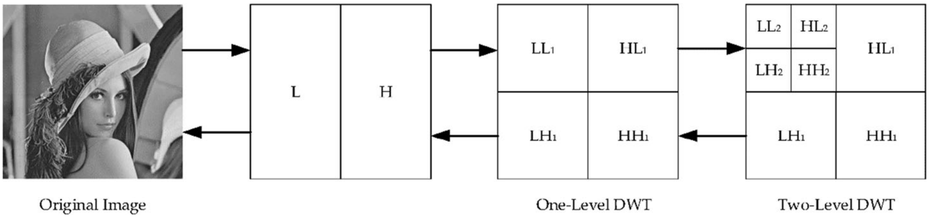


Fig. 2 DWT-1 L decomposition & DWT-2 L decomposition

stego-image S. While the extraction process inversely extracts the embedded message. Unlike classical efforts, where authors have to embed text or cipher data arbitrarily or LSB without any optimization measure, an AGA-based optimal pixel adjustment process is implemented in the proposed system. It ensures to retain maximum possible imperceptibility, quality preserve and seamless transmission even under cloud attack conditions such as RS-Analysis or Steganalysis. At first, the input medical image is processed using HAAR-DWT and split into multiple 8 × 8 blocks. Considering works of literature and allied inferences towards LSB embedding process, this approach intends to embed ciphertext in each block.

To perform embedding, at first ciphertext is transformed into an ASCII format, which is then split into S_{Text_odd} and S_{Text_Even}. The odd values S_{Text_odd} are concealed in vertical coefficients, as stated by LH2 in each of the RGB channel [50]. The even values are concealed in diagonal coefficients specified by high-level coefficients HH2 in each RGB channel [50]. The algorithm applied to perform embedding is given as follows:

```
Input: Cover Image
Output: Stego-Image
Step-1 Start the process
Step-2 Convert the secret message (say, diagnosis details) in ASCII code $S_{Text_{ASCII}}$
Step-3 Scan the image for row by row to each of red, green, and blue channels
Step-4 Assess the 2D wavelet coefficients for the 1L using HAAR filter $(LL1), (HL1), (LH1)$, and $(HH1)$ for the RGB channels
Step-5 Assess the 2D wavelet coefficients for the 2L level using HAAR wavelet filter $(LL2), (HL2), (LH2)$, and $(HH2)$ for the RGB channels
Step-6 Begin a Loop
Embed $S_{Text_{ASCII}}$ using LSB embedding concept.
Process AGA-OPAP for adaptive pixel optimization and RS-Attack resilient LSB embedding.
end loop
Return Stego-Image
End
```

To retain maximum medical image quality as well as security against online attacks such as RS-Analysis or steganalysis an AGA intends to fit $S_{TextASCII}$ in such manner that it does not lead to any substantial entropy or visual trait portentous presence of confidential data.

In the last few years, numerous attacker modules have been developed to target, detect and attack data over uncertain communication channels, such as cloud network. Amongst the significant attacks, RS-Analysis also called steganalysis has surfaced as the dominant attacker model intended to retrieve stego-information from the multimedia data communication. Before discussing the proposed AGA-OPAP based LSB embedding model, a snippet of RS Analysis or Steganalysis model is given as follows:

AGA has been applied to enhance image quality, embedding capacity, and statistical factors such as regular and singular coefficient values in each block. This approach can ensure maximum possible embedding while retaining optimal data quality and visual imperceptibility. Consequently, it can help avoid those attacks that use visual changes or statistical changes to detect hidden information or secret information within cover image during transmission. Considering RS-Analysis, also called steganalysis attack condition which employs statistical features to detect hidden information in multimedia data under transmission; the proposed model takes account of RS parameters and PSNR sensitive LSB embedding to ensure optimal data security. The detailed discussion of the proposed embedding model is given as follows:

A. RS analysis (Steganalysis) There are three distinct kinds of block flipping; Positive flipping (F_1), Negative flipping (F_{-1})and Null flipping (F_0). F_1 signifies the transformation association between the 2i and 2i + 1 pixels (say, 0–1, 2–3,…,254–255), equivalent to the LSB coefficient. Similarly, the transformation association in between 2i and 2i − 1 pixels (say, −1, −1-0, 1–2…255–256) signifies the negative flipping F_{-1}. Thus, the association between positive and the negative flipping follows (4).

$$F_{-1} = F_1(x+1)-1 \tag{4}$$

The null flipping, which stated the identity permutation follows the following condition (5).

$$F_0(x) = x \tag{5}$$

$$F(G) = \left(F_{M(1)}(x_i), F_{M(2)}(x_2), \dots, F_{M(n)}(x_n)\right) \tag{6}$$

These parameters (i.e., F_1, F_{-1} and F_0) are often called as the flipping functions. Employing these flipping functions on each pixel of the input image block the flipped group ($F(G)$) is obtained. Mathematically,

Here, we define a parameter called flipping mask M. Where $M = M(1), M(2), \dots, M(n)$, and $M(i)$ states for 1,0 and − 1.

The group G would remain constant only when $f(F(G)) > f(G)$. Similarly, G is singular when $f(F(G)) < f(G)$. To perform the RS analysis, the following mechanism is taken into consideration. At first, the input image is split into multiple non-overlapping sections or blocks where each block is re-arranged to constitute a vector G., where $G = (x_1, x_2, .., x_n)$ is ordered in specific random (say, Zigzag) manner. The correlation amongst the pixel is obtained using a discrimination function, defined in (7).

$$f(x_1, x_2, .., x_n) = \sum_{i=1}^{n-1} |x_i - x_{i+1}| \tag{7}$$

In (7), the variable x states the pixel's value, while the total number of pixels is given by n. Here, the resulting value of f signifies the spatial correlation between the neighbouring pixels.

The small value of f states the strong correlation between the adjacent pixels. Once obtaining the complete value of $f(G)$, the non-negative flipping is applied (i.e., $M(1)$, $M(2)$, …, $M(n)$) either 0 or 1. On the contrary, for non-positive flipping, we apply 0 or −1 for each input image block. Now, processing flipping over each block, estimate $f(F(G))$ for each block and thus the relative count of regular or consistent blocks after positive flipping is obtained as R_m. Similarly, the relative number of singular blocks is obtained as S_m. Similarly, for negative flipping, the regular and singular blocks are obtained as R_{-m} and S_{-m}. The total number of above-stated blocks in the raw images after performing flipping follows the following associations.

$$R_m \approx R_{-m}, S_m \approx S_{-m} \ and \ R_m > S_m, R_{-m} > S_{-m} \tag{8}$$

The difference between R_m and R_{-m} increases as per the size of embedding message. Similarly, the difference values of S_m and S_{-m} too increases with increase in embedding text. Such facts help attackers on a cloud platform or environment detect hidden information that can significantly lose data privacy. Considering it as motivation, the focus is made on developing an embedding model where the above-stated parameters (i.e., the difference between the values of R_m and R_{-m} and S_m and S_{-m} could be reduced while ensuring higher embedding capacity. This, as a solution, can accomplish attack-resilient secure cloud communication model. To achieve it, an AGA algorithm has been developed that intends to adjust pixels optimally $R_m \approx S_m$, $R_{-m} \approx S_{-m}$. The detailed discussion of the proposed AGA based OPAP is given in the subsequent section.

B. AGA based OPAP To avoid any stego-information retrieval or data attack, the focus is on achieving the condition given in (8) by performing OPAP. Here, we perform pixel adjustment to achieve a standard or natural condition defined as $\mathrm{R_m} \approx \mathrm{S_m}$, $\mathrm{R_{-m}} \approx \mathrm{S_{-m}}$. Since the variations in the bits in the higher place might violate or reduce the image quality of the stego-image, merely the 2nd and 3rd LSBs are modified. For illustration, let B as given in (9), be the original value of the input image (block). Now, in case of the strategic modification is made merely in LSB place (only 2nd LSB plane), the variation or the changes in between the original image block and the modified image block can be considered as a matrix called Adjustment Matrix (AM), given as A_1 and A_2. Thus, the modified image blocks are $B_1^{'} = B + A_1$ and $B_2^{'} = B + A_2$. For illustration, let B be the original image block while $f(B) = 99$, while $f_-(B) = 120$,where f_- states the non-positive flipping. Now for the modified image block $B_1^{'}$, $f_-\left(B_1^{'}\right) = 90$, only when F is non-positive flipping. Similarly, for $B_2^{'}$, $f_-\left(B_2^{'}\right) = 150$.

$$\mathrm{B} = \begin{bmatrix} 107 & 109 & 107 & 105 & 104 & 102 & 102 & 104 \\ 107 & 106 & 105 & 104 & 105 & 103 & 105 & 102 \\ 107 & 105 & 107 & 105 & 102 & 103 & 104 & 103 \\ 107 & 107 & 105 & 106 & 104 & 103 & 103 & 104 \\ 107 & 109 & 107 & 104 & 104 & 102 & 103 & 102 \\ 104 & 107 & 106 & 103 & 103 & 104 & 102 & 100 \\ 110 & 109 & 109 & 105 & 105 & 105 & 105 & 102 \\ 109 & 109 & 109 & 106 & 104 & 105 & 105 & 104 \end{bmatrix} \tag{9}$$

$$\mathrm{A}_1 = \begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{10}$$

$$\mathrm{A}_2 = \begin{bmatrix} 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \end{bmatrix} \tag{11}$$

Summarily, the kind of block (i.e., regular or singular) can be modified by changing or making a suitable adjustment. In such cases, adjusting the pixels optimally, RS-Analysis attack of steganalysis attack can be avoided on the cloud environment. An Adaptive Genetic Algorithm (AGA) is applied to achieve it, which obtains the Optimal Adjustment Matrix (OAM) to ensure minimum disparity amongst the values of regular and singular image blocks. A snippet of the AGA based OPAP method and resulting OAM estimation is discussed in the subsequent section.

GA is a nature-based EC model, which employs Darwin's principle of survival to obtain the optimal or sub-optimal solution after a defined number of generations. Functionally, it applies the concept of human evolution to obtain an optimal solution by transforming an optimization of search problem into the phenomenon of chromosome evolution. Processing the evolution concept, once it achieves an optimal or the best solution after iterating a predefined number of generations (or, stopping criteria), the optimal solution obtained is presented as the final solution of that problem. Functionally, GA employs the processes named Population Generation, Crossover and Mutation. In practice, the adaptive values influence the copy operation, and an individual with significantly high fitness value is considered for the next generation. A candidate solution's fitness value signifies its maximum likelihood of becoming selected for breeding in the next generation. To reduce computational overheads caused due to increase search space, the mutation process is applied that drops the individual with minimum fitness value, and such individuals are not carried forward for crossover in the next generation. Once embedding the secret data within the cover image using LSB embedding, we execute AGA-OPAP. A snippet of the applied AGA-OPAP is given as follows:

In the proposed LSB embedding method, the stego-image is split into 8 × 8 blocks, where each block is categorized and labelled by applying the following mechanisms.

Step-1: Let the image block be B, then for B implement the non-positive flipping F_{-} as well as non-negative flipping F_{+}.

Step-2: Generate the flipping mask M_{+} and M_{-}, randomly and obtain the results $B^{'}_{+}$ and $B^{'}_{-}$.

Step-3: With the obtained value of $B^{'}_{+}$ and $B^{'}_{-}$, estimate the values of $f\left(B^{'}_{+}\right)$, $f\left(B^{'}_{-}\right)$ and $f(B)$.

Step-4: Process the steps 1, 2 and 3 iteratively for 1000 number of generations and define four distinct variables to classify the blocks by comparing $f\left(B^{'}_{+}\right)$, $f\left(B^{'}_{-}\right)$ and $f(B)$.

P_{+R}, it states the number of occurrences when the block remains regular under the non-negative flipping,

P_{+S}, it states the number of occurrences when the block remains singular under the non-negative flipping,

P_{-R}, it states the number of occurrences when the block remains regular under the non-positive flipping.

P_{-S}, it states the number of occurrences when the block remains singular under the non-positive flipping.

Step-5: Perform P_{+R} to P_{+S} and P_{-R} to P_{-S} and perform labelling of the image blocks as per the following conditions:

$R+$, if $\frac{P_{+R}}{P_{+S}} > 1.8$.

$S+$, if $\frac{P_{+S}}{P_{+R}} > 1.8$

$R-$, if $\frac{P_{-R}}{P_{-S}} > 1.8$

$S-$, if $\frac{P_{-S}}{P_{-R}} > 1.8$

Step-6: Classify blocks into four distinct groups, $R+R-$, $R+S-$, $S+R-$, $S+S-$. Ignore the blocks, not a part of above-stated types.

Step-7: Perform the comparison of the original input image, the magnitude of $R+R-$ and $S+R-$ blocks, which often shows increased in stego-images.

Such increase in the above-stated parameter can be detected using RS Analysis, which can be used as the intrusion tool to attack that specific multimedia data to get unauthorized access of the stego-image and hidden information. Considering the above-stated fact and motive to alleviate the distinguishable or perceptible disparity between the values of $+-$ and $+-$ blocks, this research applies the AGA algorithms to decrease the value of $R-$ blocks. The implementation of AGA-based OPAP comprises three essential functions: initialization (population initialization), crossover, and mutation. The procedures involved in AGA-OPAP optimization and allied pixel adjustment is detailed as follows:

4 Population initialization

The initial pixel, or the first pixel, chose three adjacent pixels in each image block as the initial chromosome (Fig. 3).

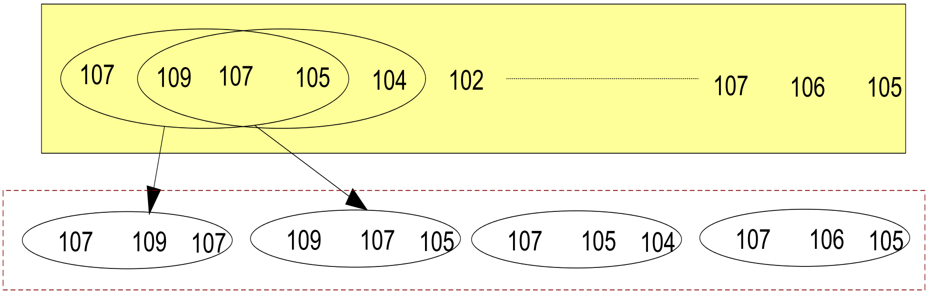


Fig. 3 Selection of the chromosomes

5 Reproduction and mutation

Perform flipping of the second least bits in the chromosomes arbitrarily and generate the (second generation) chromosomes C_i.

6 Selection

Estimate the fitness value of each chromosome and select the best chromosome using (12).

$$Fitness = \alpha(e_1 + e_2) + PSNR \tag{12}$$

In (12), the variable e$_1$ states the likelihood of f(F$_-$(C$_i$)) < f(C$_i$). Similarly, e$_2$ signifies the likelihood of f(F$_+$(C$_i$)) > f(C$_i$). The variable PSNR signifies the Peak Signal to Noise Ratio of the participating chromosome, while ∝ presents a weight parameter which has been obtained empirically. Mathematically, PSNR has been obtained using (13).

$$PSNR = 10\log_{10}\frac{M \times N \times 255^2}{\sum_{i,j}\left(y_{i,j} - x_{i,j}\right)^2} \tag{13}$$

In (13), M and N signify image dimension while x and y state the image intensity before and after embedding. Here, α states a weight parameter which controls the visual quality of the input multimedia data and secrecy of the secret text. For a specific value of α, higher the values of $e_1$and e_2, we hypothesize to achieve higher data security. Hence, in the proposed model, optimizing (specifically maximizing) the value of (13) (say, fitness value) has been considered as the fitness function. In our proposed method, we ensure maintaining $e_1$and e_2 higher than a threshold, which is experimentally decided. We have applied the threshold as 0.8.

1. **Estimate** P_{-R} and P_{-S} of the neighbouring image block and check whether $P_{-S} > P_{-R}$. If so, the block is considered as successfully adjusted.

2. **Crossover** In the crossover process, shift the chromosome by one pixel and reinitiate step-2. Once performing crossover twice, stop the cycle.

This overall process is called OPAP, making hybrid cryptography and steganography more resilient to attacks such as RS Analysis or steganalysis, achieving optimal security over the cloud platform. Now, once all image blocks are successfully adjusted, estimate the value of R_m, R_{-m}, S_m and S_{-m} of the image and in case the disparity of $\mathrm{R_m}$ and R_{-m} (and, S_m and S_{-m}) is more than 5%, perform adjustment of the next or the sub-sequent image blocks. In the proposed model, each block is labelled before initiating OPAP, and thus, we reduce computational overheads significantly. Furthermore, AGA's use reduces the exhaustive search operation and achieves computational efficiency, making it suitable for secure medical data transmission over cloud infrastructure.

6.1 Secret data extraction

Once embedding the data inside the cover image and obtaining the stego image, it is transmitted over cloud communication channels. Receiving the data at the receiver end, we have obtained confidential data and original cover image by performing extraction using the 2D-DWT-2 L method.

Figure 4 illustrates the procedure of extracting encrypted text from the images. This process will begin after the successful completion of the decomposition of images using DWT-2 L. The extraction algorithm is described below

.

```
Input: Stego Image
Output: Secret message, Cover image.
Initiate the process
Step-1 Scan the stego image row-by-row for the red, blue and green channels
Step-2 Assess the 2D wavelet coefficients for the 1-level of HAAR wavelet filter for the RGB channels
Step-3 Assess the 2D wavelet coefficients for the 2-level of HAAR wavelet filter for the RGB channels
Step-4 Formulate message " "
Step-5 Start a loop
Perform extraction of the text embedded in vertical coefficients and assign odd values =$LH2(x,y)$ in the RGB channels
Perform extraction of the text embedded in horizontal coefficients and assign even values =$HH2(x,y)$ in the RGB channels
Step-6 Close loop
Step-7 Restructure message $msg = append(odd, even)$
Step-8 Perform $IDWT$ to generate the original cover image
Step-9 Return text message as retrieved secret message and cover image.
End
```

Once extracting the text data from the images, it is reconstructed employing IDWT technique for 2nd level followed by 1st level. Figure 4 elucidates the DWT synthesis process.

Considering the need to decrypt the secret text data from the cover image, similar to the encryption phase, the hybrid scheme applies AES and RSA algorithms to decrypt the receiver's confidential data. Receiving the stego image at the receiver unit, we decrypt the text using a private key to obtain the original secret message transmitted. The decryption algorithm used to retrieve the original secret data is given as follows:

```
Input: Ciphertext received $Cipher\ _{Tx}$, key
Output: Secret message.
Initiate the process
Step-1 Split the received ciphertext into two components; $HashedText$ and $HashedKey$
Step-2 $Enc\_msg$= decompress($HashedText$)
Step-3 $Enc_{Key}$=decompress($HashedKey$)
Step-4 $x$=decrypt_AES-256($Enc_{Key}$, $s$)
Step-5 $Enc\_S_{Text\_odd} = split(Cipher\ _{F_{Total}}, S_{Text_{odd}})$
Step-6 $Enc\_S_{Text\_Even} = split(Cipher\ _{F_{Total}}, S_{Text_{Even}})$
Step-7 $S_{Text\_odd}$=$decrypt\_AES - 256(Enc\_S_{Text\_odd}, s)$
Step-8 $S_{Text\_Even}$=$decrypt\_RSA(Enc\_S_{Text\_Even}, x)$
Define plain text message
Step-9 Initiate loop for all characters
If odd
Insert odd characters into odd indices within the plain text message
else
Insert even characters into even indices within the plain text message.
End loop
Step-10 Return original secret text and image transmitted.
End
```

By implementing the above-stated approach, a robust and computationally efficient model strengthened by employing hybrid encryption enhancement and attack resilient (for example, steganalysis or RS-Attack), Visually Imperceptible model is developed. The proposed system can secure medical data transmission over different environments while ensuring optimal performance. The detailed discussion of the simulation results and its inferences is given in the subsequent section.

7 Results and discussion

Considering the exponential increase in cloud-based secure medical data communication, this research focused on developing a hybrid encryption strategy combining cryptography and steganography that provide data privacy. The overall proposed model is developed using MATLAB 2018a tool, which has been simulated with the computer specifications of 2.27 GHz Intel (R) Core (TM), 3rd generation processor (I3 CPU), 8 GB RAM and

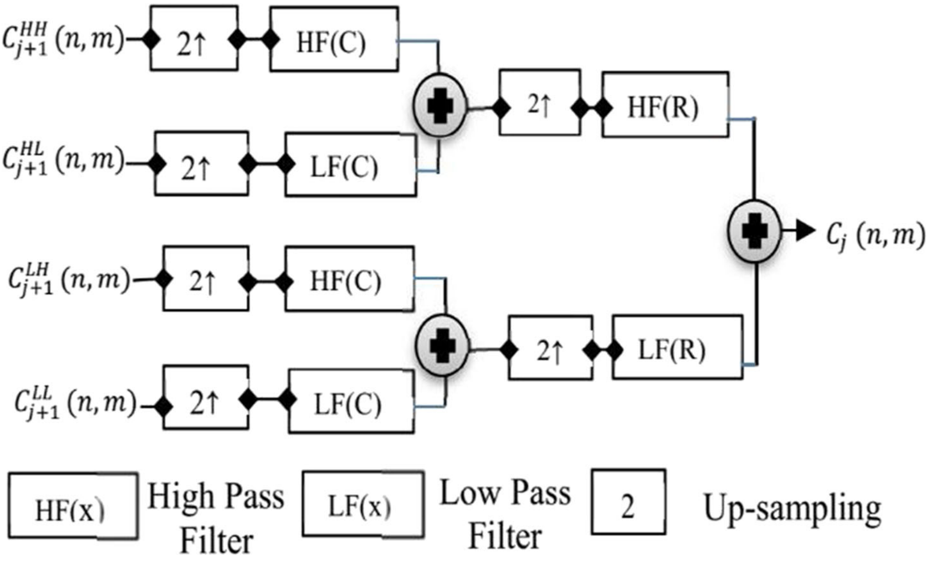


Fig. 4 Extracting encrypted text from images showing the procedure of synthesis of DWT-2 L.

Windows-7 operating system. Multiple images as the cover image and secret message of varied sizes are employed to assess the proposed model's performance.

The Hybrid encryption and Steganography model can be useful or more efficient when it fulfils the following:

7.1 Histogram analysis

As stated in Table 1, minimizing histogram pattern variations before and after message embedding in the cover image can reduce visual perception or result tracking by attackers. Histogram variations occur due to increased entropy within the cover image due to text embedding, and therefore to retain visual imperceptibility reducing entropy through optimal pixel adjustment is vital. To achieve it, an AGA-OPAP based LSB embedding resulted in minimum histogram variations (Table 2). As depicted in Table 2, the proposed model exhibits negligible or near-zero variation in histogram after message embedding, supporting the visual imperceptibility aspect for secure communication.

To assess the efficacy of the proposed model, in this work we considered standard benchmark images such as Baboon, Lena, Baboon, Sailboat, Peppers, Female [19] [33] (*.jpg) as well as the medical images [56] (DRISHTI-GS dataset in *.png). Here, the prime objective was to assess whether the proposed method can be adequate or suitable for the healthcare application environment. Since in healthcare images retaining image-quality and the inherent feature is of utmost significance, we have applied critical healthcare data of "Diabetic Retinopathy", where even a single nerve can have important diabetes information. Introduction of additional text (secret) data could cause entropy and hence quality degradation. However, the proposed model intended to optimize such entropy and ensure that stego-image (image after embedding) retains maximum possible image quality and originality. Observing the results, it can be found that the proposed method achieves optimal performance in terms of visual imperceptibility. It can avoid numerous attack scenarios online in the cloud

Table 1 Performance criteria

S.No.	Parameter	Definition
1.	PSNR	To preserve the image quality even after embedding secret text data, PSNR should be higher. The significant reduction in PSNR value can depict certain hidden information that can trigger attacker models to target and attack the transmission data.
2.	Entropy	It signifies the disturbance in the original image. To ensure minimum perceptibility, the model requires maintaining minimum entropy after message embedding. The minimum value of entropy can avoid getting attention from attacker modules.
3.	Embedding Capacity	It signifies how the secret text data can be embedded per unit of the cover image. The model can be superlative or better if it ensures or maintains higher embedding capacity without introducing significant entropy and PSNR reduction (in addition to the regular and singular coefficient changes in RS analysis.
4.	Changes in Regular coefficients ($\boldsymbol{R_m}-\boldsymbol{R_{-m}}$))	It signifies the variation or the difference between the regular coefficient before and after embedding. Higher differences are the indicator for hidden information which invites attackers such as RS attacker or steganalysis attacking modules to target data under the transmission. Lower the differences, higher the imperceptibility and resulting data security.
5.	Changes in Singular coefficients ($\boldsymbol{S_m}-\boldsymbol{S_{-m}}$)	It signifies the variation or the difference between the singular coefficient before and after embedding. Higher differences are the indicator for hidden information which invites attackers such as RS attacker or steganalysis attacking modules to target data under the transmission. Lower the differences, higher the imperceptibility and resulting data security.
7.	Histogram Variations	It signifies the different histogram patterns of the cover image and stego image, before and after the embedding. Lower or negligible histogram graph variations show near-optimal embedding, which supports imperceptibility and hence attack resilience.

environment. To simulate the proposed model for performance verification, random text information such as a snippet of common test sentences such as “My Own Address”, “My Personal Biography” with different sizes (in notepad, *.txt) was applied. Due to space constraints and inferior significance of text (embedding data) details, we have not mentioned it in this manuscript. Dataset images (Table 2) are the cover images considered for the simulation and performance assessment.

7.2 PSNR assessment

It is calculated to measure the quality of images created by Peak Signal to Noise Ratio (PSNR) compression. If it produces a high PSNR value, the compression technique is considered significant, which means that the error is deficient and the reconstructed error is minimal. The image seems to be very similar to the original image. When the PSNR value is between 30 and 50 dB, lossy image quality is considered acceptable. The quality of the image is considered

Table 2 Histogram Pattern Analysis

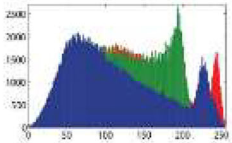
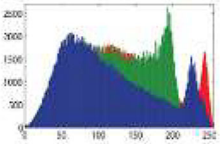
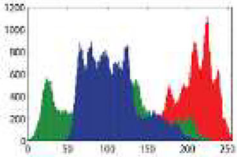
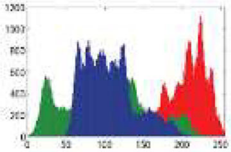
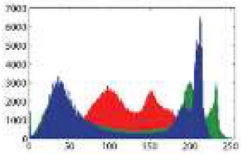
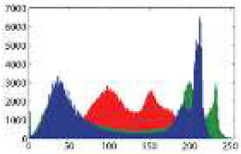
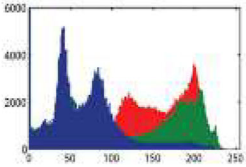
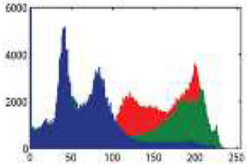
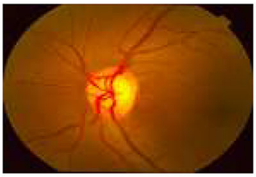
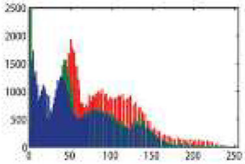
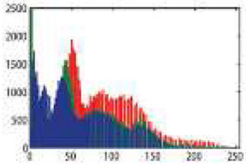
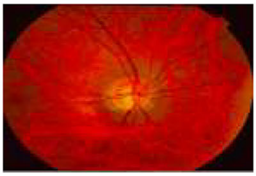
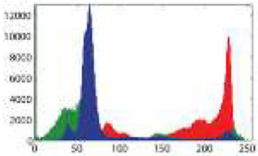
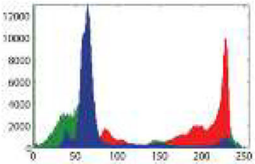
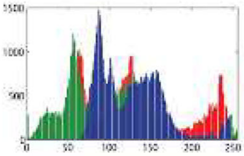
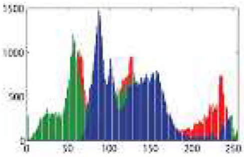
Name	Dataset	Histogram of the cover image	
		Before	Post Embedding and OPAP
Baboon			
Lena			
Sailboat			
Peppers			
Retina1			
Retina2			
Female			

Table 3 PSNR Performance (for 250 bytes of text data)

Dataset	PSNR (dB)		
	Before	Post Embedding	Post Optimization
Baboon	35.0600	31.9200	34.0053
Lena	37.4873	35.8762	36.5852
Sailboat	33.1850	30.7611	31.2970
Peppers	37.2667	33.0110	34.1010
Retina1	43.3450	41.2101	42.8701
Retina2	46.8071	44.0629	45.6255
Female	35.6216	33.3414	34.3060

ideal if the PSNR value is above 40 dB. The compression technique is highly not appropriate if the PSNR value is below 20 dB.

Table 3 presents the PSNR performance of the proposed model for 250 bytes in text (secret data) embedding. Observing the result in Table 3, where the PSNR has been obtained for the text embedding size of 250 bits, it can be found that after embedding the text or secret data, the PSNR decreases; however, the contribution goes to the proposed AGA-OPAP assisted LSB embedding method, which improves the message embedding and even optimizes the PSNR. Interestingly, observing PSNR performance, the proposed model either achieves near original PSNR or even improves the image quality, which results in improved PSNR value (post-embedding and OPAP optimization). The mathematical model for PSNR estimation was applied in (13) for the image processed after 2D-DWT-2 L and post-AGA-OPAP optimization. The results obtained (Table 4) reveals that the proposed AGA-OPAP assisted LSB

Table 4 PSNR performance over different sizes of the secret text data

Dataset	Data Size (bytes)	PSNR (dB)		
		Before	Post Embedding	Post Optimization
Baboon	250	35.0600	31.9200	34.0053
	500	38.8630	36.2003	37.8942
	1000	36.7491	35.8990	36.1804
Lena	250	37.4873	35.8762	36.5852
	500	33.1041	32.0072	32.9183
	1000	35.4901	34.0700	35.1003
Sailboat	250	33.1850	30.7611	31.2970
	500	36.8931	35.4180	35.9814
	1000	36.2443	35.0134	35.9993
Peppers	250	37.2667	33.0110	34.1010
	500	32.2442	31.6320	32.1248
	1000	38.0012	37.4021	37.8732
Retina1	250	43.3450	41.2101	42.8701
	500	49.1251	47.3427	48.6391
	1000	48.8422	46.1120	48.1297
Retina2	250	46.8071	44.0629	45.6255
	500	46.0367	43.6730	44.9834
	1000	44.5259	42.1147	43.5895
Female	250	35.6216	33.3414	34.3060
	500	38.8736	36.5290	37.9201
	1000	37.9910	36.3019	37.1003

embedding method is of utmost significance towards retaining and optimizing image quality for quality-centric communication over the cloud environment.

7.3 Entropy analysis

As an image security operation, the cipher generation is performed, which will increase the image input disturbances. Consequently, this can lead to a surge in image entropy that degrades the quality of the image and broadens the horizon for intruders to target specific data. On the other hand, to make it difficult for the attacker to differentiate the encrypted data and the original image information, encryption imposes additional information on the image. In such instances, it is vital for preserving the optimum entropy of the data being transmitted. With this strategy, the encrypted image data's entropy is quantified with Eq. (14).

$$ENT(I) = -\sum_{i=1}^{2^8} P(I_i)\log_b P(I_i) \tag{14}$$

In (14),*ENT*(*I*) states the entropy of an image, where I signify the intensity and $P(I_i)$ signifies the probability of the intensity value I_i.

Observing the above results (Table 5), it can easily be visualized that the increase in entropy is significantly low and therefore retains the image quality. It affirms the encrypted images' suitability for critical applications such as healthcare (telemedicine) or critical data communication purposes.

7.4 Embedding capacity analysis

The embedding capacity signifies the extent or the percentile to which a unit image can embed the text data (i.e., ensuring no reduction in PSNR and correlation, and maintaining low entropy). Table 6 presents the embedding capacity performance by the proposed model.

Observing Table 6, it can be easily found that the proposed method accomplishes significantly large enhancement in the embedding capacity post-optimization. This can be because of the proposed OPAP concept's robustness, which ensures optimal embedding while retaining entropy low and PSNR high, the employed AGA heuristic model's key objectives. Thus, the results obtained signify the proposed model's suitability for sizeable scale-sized encryption and secure communication purposes. The addition of more secret information (text data) in the image might impose high entropy that eventually could reduce image quality (i.e., PSNR). In such a case, it is significant to assess whether the inclusion of the proposed AGA-

Table 5 Image entropy analysis

Dataset	Initial Image Entropy	Entropy (Post-embedding)
Baboon	6.3510	7.9898
Lena	5.4312	7.9958
Sailboat	6.0468	7.9053
Peppers	6.1031	7.8998
Retina1	7.3904	7.6730
Retina2	7.4938	7.9968
Female	7.1020	7.9993

Table 6 Embedding capacity analysis

Dataset	Embedding capacity (%) (post 2D-DWT-2 L embedding)	Embedding capacity (%) (Post-AGA-OPAP optimization)
Baboon	13.01	46.90
Lena	10.20	47.81
Sailboat	10.91	35.01
Peppers	17.99	48.84
Retina1	12.04	57.90
Retina2	10.01	59.99
Female	19.93	56.91

OPAP assisted LSB embedding helps retaining maximum possible image quality even after extensive secret data embedding. In this paper, we assessed the performance for the different sizes of the secret text data embedded in the cover image with this motive. Observing the results (Table 4), it can easily be found that though with an increase in secret data size (to be embedded into image), the PSNR decreases; however, our proposed AGA-OPAP based LSB embedding method reduces entropy and retains better PSNR. It affirms that the proposed method can achieve optimal PSNR irrespective of the data size. The results affirmed that the inclusion of AGA-OPAP could be vital to ensure higher data embedding inside the medical image without imposing any significant quality degradation or visual traits, which might invite intruders to attack over uncertain cloud communication channels allied network.

7.5 Regular and singular coefficient analysis

The attack models such as RS-Attack or Steganalysis attack might explore the medical data under the transmission to attack the specific data-carrying certain significant information or secret information. The variations in regular and singular coefficients per block of the image are examined to alleviate such issues. As stated in Table 1, higher differences in the regular and singular coefficients can reveal the attackers about the presence of private data within the multimedia data, and therefore maintaining lower difference can be advantageous.

Observing Table 7, it can be found that the proposed method achieves relatively lower differences in regular coefficient value ($R_m - R_{-m}$) and the singular difference value($S_m - S_{-m}$).

Table 7 RS analysis (secret data size 250 bytes)

Dataset	RS Parameters					
	Regular Coefficient Difference ($R_m - R_{-m}$)			Singular Coefficient Difference ($S_m - S_{-m}$)		
	Before	Post Embedding	Post Optimization	Before	Post Embedding	Post Optimization
Baboon	0.0063	0.0054	0.0057	0.0029	0.0015	0.0087
Lena	0.0035	0.0025	0.0031	0.0006	0.0112	0.0008
Sailboat	0.0039	0.0054	0.0065	0.0066	0.0015	0.0054
Peppers	0.0091	0.0074	0.0076	0.0089	0.0076	0.0059
Retina1	0.0029	0.0025	0.0034	0.0043	0.0112	0.0004
Retina2	0.0039	0.0077	0.0019	0.0002	0.0073	0.0062
Female	0.0081	0.0026	0.0056	0.0031	0.0108	0.0038

It reveals that the proposed method can achieve a high level of visual imperceptibility to secure medical data communication over a cloud channel.

7.6 Encryption and decryption speed analysis

To assess the time efficiency of the proposed model for encryption is calculated using MATLAB functions *($tic - toc$). The execution time consumed over the different dataset is given in Table 8.

Observing the above-stated results, it can easily be found that the proposed system consumes low execution time, including both encryption as well as decryption, which exhibit its robustness towards time-efficient computation.

7.7 NCPR and UACI test

In addition to the visual and statistical characterization discussed above, we have analyzed our proposed security model's effectiveness in Number of Changing Pixel Rate (NCPR) and the Unified Average Channel Intensity (UACI). High NPCR and UACI value usually imply higher randomness and therefore, high tolerance against any differential attack probability [63]. The randomness test results with a higher NCPR value confirm the proposed system's attack resiliency's essence. Similarly, via our proposed medical data security model, UACI also confirms satisfactory results. The thorough discussion of NCPR and UACI conditions during encryption for image randomness can be found in [63].

Recalling the overall design where the fundamental goal of employing hybrid encryption with AGA-OPAP was to avoid any attack conditions such as Man-In-The-Middle attack (MITM), steganalysis or linear and differential based attack approaches since the proposed model avoids providing any scope of visual perceptibility and maintains low entropy, high PSNR, it would be able to resilient any attack conditions. Tables 9 display NPCR and UACI values for the images.

7.8 Mean absolute error analysis

To determine the receiver side's image quality, we used Mean Absolute Error (MAE) to evaluate accuracy (15).

Table 8 Execution time over of the secret text data (250 bytes)

Dataset	Data Size (bytes)	Execution Time (seconds)	
		Encryption	Decryption
Baboon	250	12.97	14.01
Lena	250	12.45	14.00
Sailboat	250	12.40	14.91
Peppers	250	11.31	14.92
Retina1	250	12.83	14.31
Retina2	250	12.01	14.89
Female	250	12.88	14.87

Table 9 NPCR and UACI randomness test

Dataset	NPCR (%)	UACI (%)
Baboon	99.6057	28.7671
Lena	99.7345	36.5632
Sailboat	99.7576	33.8148
Peppers	99.7942	36.6581
Retina1	99.7464	36.6070
Retina2	99.7398	36.5610
Female	99.7672	33.3847

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left(\left|Y_i^{'} - Y_i\right|\right) \tag{15}$$

where $Y_i^{'}$refers to the calculated output, while Y_i states for the expected value. The results obtained for inputs (with 250 bytes of text input) are given in Table 10. The results (Table 10) signifies the robustness in terms of very negligible error profile, which undoubtedly affirms its superior image quality (post-decryption).

7.9 Bit error rate (BER), structural similarity (SSIM), structural content (SC) and Correlation analysis

a) **Bit Error Rate (BER):**

BER calculates the error rate of the transformed bits. This variance can be attributed to the attenuation noise or other disturbances. Eq. 16 is used to test BER.

$$BER = \frac{E}{\#Bits} \tag{16}$$

Where E indicates errors.

b) **Structural Similarity (SSIM):**

The structural similarity of images is calculated using SSIM. Here, we used the SSIM value to evaluate the similarity of the cover and steganographic images. Eq. (17) is used to construct the SSIM estimation.

Table 10 MAE performance with different input (250 bytes of the text secret data)

Dataset	MAE (%)
Baboon	0.1842
Lena	0.0963
Sailboat	0.3103
Peppers	0.3206
Retina1	0.4087
Retina2	0.1559
Female	0.1794

$$\mathrm{SSIM} = \frac{2\times\mu(\rho 1)\cdot\mu(\rho 1)+C_1}{\mu(\rho 1)^2+\mu(\rho 2)^2+C_1}\times\frac{2\times\mathbf{C}(\rho)+C_2}{\sigma_1(\rho)^2+\sigma_2(\rho)^2+C_2} \tag{17}$$

Where μ and σ are mean and standard deviation, respectively.

c) **Structural Content (SC):**

The resemblance between the cover and the steganographic image is assessed using SC. Eq. (18) to calculate the SC value.

$$SC = \frac{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(C_{ij}\right)^2}{\sum_{i=1}^{|N|}\sum_{j=1}^{|M|}\left(O_{ij}\right)^2} \tag{18}$$

Where C and O represent cover and original images.

d) **Correlation:**

The similarity and disparity between the magnitude and the data phase are determined by correlation. Equation (19) is used to determine the correlation.

$$Corr = \frac{X\cdot\sum O.S - \sum O\sum S}{\sqrt{X\left(\sum O^2\right)-\left(\sum O\right)^2}\sqrt{X\left(\sum S^2\right)-\left(\sum S\right)^2}} \tag{19}$$

X denotes the pairs in the data, the original image is O, and the steganographic image is S.

Table 11 BER, SSIM, SC and correlation of images

Dataset	Text Size(byte)	BER	SSIM	SC	Correlation
Baboon	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Lena	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Sailboat	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Peppers	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Retina1	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Retina2	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1
Female	250	0	1	1	1
	500	0	1	1	1
	1000	0	1	1	1

Table 12 Histogram of original image and post embedding of dark quality

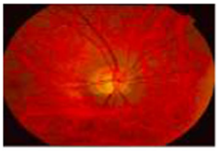
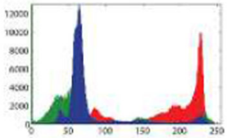
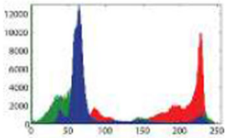
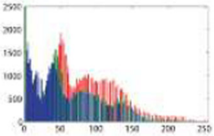
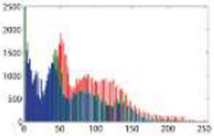
Name	Image	Original image Histogram	Histogram of post embedding and optimization
Retina[58]			
Zelda [52]			

Table 11 displays the BER, SSIM, SC and Correlation values of the images. These findings have shown that the proposed model has the potential to transmit secure medical data.

7.10 Dark and bright tone classification of images

The plain image, a histogram of the plain image and an encrypted image (post embedding and optimization) from an image of dark quality are shown in Table 12. The results show that the histogram retains similar visual quality for both the plain and cipher image.

The plain image, a histogram of the plain image, and an encrypted image (post embedding and optimization) from a bright image are presented in Table 13. The results show that the histogram retains similar visual quality for both the plain and cipher image.

Table 13 Histogram of original image and post embedding of bright quality

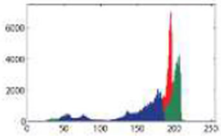
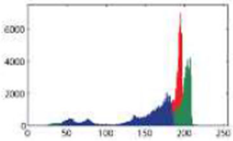
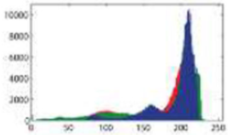
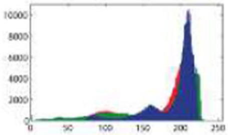
Name	Image	Original image Histogram	Histogram of post embedding and optimization
Jelli_Beans[52]			
Airplane[61]			

Table 14 Correlation coefficients based on the classification of image data quality (256 × 256)

Characteristic	Name	Red Channel			Green Channel			Blue Channel		
		Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Dark	Retina2	−0.0048	−0.0005	0.0007	−0.0016	0.0024	0.0012	−0.0032	−0.0058	0.0032
Bright	Jelli_Beans	0.0002	−0.0133	0.0002	0.0046	0.0022	−0.0021	0.0008	0.0068	−0.0006
High Contrast	Lena	−0.0021	0.0025	−0.0011	−0.0058	0.0027	−0.0024	0.0053	0.0075	−0.0037

Table 15 Correlation coefficients based on the classification of image data quality (512 × 512)

Characteristic	Name	Red Channel			Green Channel			Blue Channel		
		Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Dark	Zelda	−0.0014	0.0031	0.0013	0.0038	−0.0066	0.0079	−0.0031	0.0028	0.0053
Bright	Airplane	0.0002	−0.0133	0.0002	0.0046	0.0022	−0.0021	0.0008	0.0068	−0.0006
High Contrast	Female	−0.0059	0.0031	−0.0083	0.0061	−0.0011	0.0052	−0.0039	−0.0107	0.0070

Table 16 Result based on PSNR (dB)

Image	[7]	[30]	[11]	[38]	[61]	[8]	[14]	[33]	[13]	Proposed
Retina	56.76	57.02	46.06	74.69	45	58.96	57.02	56.34	60.8	74.92

7.11 Correlation analysis between adjacent pixels

To calculate the intensity of the linear relationship between two random variables, correlation is used. In a random image, the correlation value between neighbouring pixels is zero. Image encryption aims to render the association of neighbouring pixels close to zero in the encrypted image. The colour-encrypted image pixel correlation coefficient is determined between two horizontally adjacent pixels, two vertically adjacent pixels, and two diagonally adjacent pixels on each colour channel. The correlation coefficient values for the horizontal, vertical and diagonal components in the red, green and blue image channels are shown in Table 14 and Table 15.

7.12 Comparative assessment

The proposed model's accuracy is verified against state-of-the-art techniques where these algorithms [7, 8, 11, 13, 14, 30, 33, 38, 61] have been built to secure the healthcare data. The comparison of PSNR values with existing models is shown in Table 16. The proposed model for the security of medical data exhibited a better PSNR.

The comparison of the entropy values of the established model with existing models is provided in Table 17. The entropy value of the model designed is marginally better than the developed methods of Nithya et al. [11] focused on securing images in cloud storage environments with an integrated security framework using the DNA coding and image encryption methods to provide heightened security, Emy et al. [50] proposed an approach for improving the security of the colour image data by distributing the symmetric keys, Gupta et al. [15] employed Compressed Hybrid Cryptosystem that constitutes compression, encryption and secure session key exchange along with the transmission of image and Zhang et al. [68] proposed a new image compression and encryption scheme based on the nearest-neighbouring coupled-map lattices (NCML) and Non-uniform Discrete Cosine Transform (NDCT).

Table 18 portrays the comparison of Embedding Capacity Analysis (%) of the proposed model against existing models, where the results are better than the state-of-the-art approaches of Mansour et al. [29] and Ou et al. [36] where an efficient adaptive embedding and optimization of colour images is proposed.

Table 19 displays the proposed method's overall processing time for encoding and decoding information on the sender and recipient's end, respectively. The results demonstrate

Table 17 Results based on Entropy Values

Image	[11]	[50]	[15]	[68]	Proposed
Lena	7.9030	7.9955	7.9839	–	7.9958
Baboon	7.9020	7.9989	–	7.9952	7.9898

Table 18 Comparison based on embedding capacity

Image	[29]	[36]	Proposed
Lena	47.70	46.67	47.81
Baboon	36.17	38.42	46.90
Peppers	45.79	46.21	48.81

Table 19 Comparison based on encryption and decryption speed

Image	Time (Second)	[11]	[50]	[61]	Proposed
Baboon	Encryption	–	12.53	–	12.97
	Decryption	–	14.93	–	14.01
Lena	Encryption	22.53	12.21	86.012	12.45
	Decryption	20.56	14.69	86.547	14.00
Sailboat	Encryption	–	12.51	–	12.40
	Decryption	–	14.82	–	14.91
Peppers	Encryption	22.58	12.39	–	11.31
	Decryption	20.42	14.78	–	14.92

that the proposed method can better perform the state-of-the-art methods [11, 50, 61] for colour images.

The comparative NPCR and UACI values from the model built with the three previous research models are shown in Tables 20. All image data tested from the developed cryptographic method for NPCR and UACI values are higher than the previous studies of [50], seyedzadeh et al. [51], Niyat et al. [64] and Ahmad et al. [3] incorporates color image encryption algorithm based on chaotic system and cellular automata. It can be inferred based on the test results that the improved cryptosystem model is safer against differential attacks.

Table 21 shows the correlation coefficients between the proposed model and other cryptosystem models in each colour channel. The correlation value is closer to zero for the proposed model than for the model by Ref. [68] where a new algorithm for image compression and encryption based on spatiotemporal cross chaotic system is proposed.

Thus, considering the proposed model and its simulation-based performance, it can be inferred that the proposed system achieves optimal efficiency, which makes it suitable for secure medical data communication over the cloud environment. Observing the overall results, it can be found that the use of hybrid encryption (AES and RSA together) and AGA-OPAP

Tables 20 Result analysis of NCPR and UACI values

Image	Values	[50]	[51]	[64]	[3]	Proposed
Baboon	NPCR	99.7457	99.6823	99.6378	99.5830	99.6057
	UACI	38.2023	33.5031	33.4673	33.6110	28.7671
Lena	NPCR	99.7470	99.6827	99.6525	99.6450	99.7345
	UACI	36.7368	33.4898	33.4331	33.5610	36.5632
Sailboat	NPCR	99.7500	99.6847	–	99.5580	99.7576
	UACI	38.5050	33.5115	–	33.4830	33.8148
Peppers	NPCR	99.7509	99.6818	99.6254	99.6140	99.7942
	UACI	34.7577	33.5308	33.4566	33.5870	36.6581

Table 21 Comparison based on Correlation of RGB Channels

Ref.	Image	Red Channel			Green Channel			Blue Channel		
		Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
[68]	Lena	0.0259	0.0213	0.0562	0.0256	0.0143	0.0724	0.0259	0.0166	0.0602
Proposed	Lena	−0.0021	0.0025	−0.0011	−0.0058	0.0027	−0.0024	0.0053	0.0075	−0.0037

based embedding optimization can yield an optimal solution for secure medical data communication over the cloud platform. Similarly, results indicate that RSA-64 and AES-256 as a strategically combined solution can be better towards the proposed model, though in this study we have not performed individual performance assessment for RSA and AES (distinctly). Results obtained (Tables 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21) confirm that the use of AGA-OPAP has strengthened the proposed model to achieve optimal pixel adjustment, which eventually yielded PSNR enhancement, minimum histogram changes or entropy. It has also helped (due to PSNR and RS sensitive optimization) achieving optimal Regular and Singular coefficient values of each block. The simulation results reveal that the use of AGA-OPAP based LSB embedding has achieved maximum possible visual imperceptibility and data (image) quality which affirm suitability of the proposed model for the cloud environment.

Observing the overall results and corresponding inferences, it can be inferred that proposed model can enable an optimal security solution for the different cloud purposes, including Electronic Healthcare Records (EHR), Tele-medicine, critical image and allied annotation information hiding for future (security) purposes. Contemporarily, a large number of cloud applications provide data security, and undeniably our proposed model can be of great significance to support them, either as a standalone security solution or as a plug-in or Application Program Interface (API). The overall research conclusion is given in the subsequent sections.

8 Conclusion

Considering the exponential rise of medical data communication over the cloud environment, which is often considered uncertain, in this research, the emphasis was made on developing a robust and efficient secure data transmission model. The proposed model utilizes cryptographic and steganography features to introduce security and quality-centric data transmission. The use of hybrid encryption (AES and RSA) and their strategic implementation towards secret data encryption and decryption strengthened the overall security level and ensured that the secret information could not be retrieved easily. On the other hand, realizing the quality preserve aspect of steganography which is often used in medical data security, an Adaptive Genetic Algorithm based OPAP was developed that optimized least significant bit embedding over image-blocks. The AGA-OPAP model considered PSNR and Regular and Singular Coefficient values per block of the image as objective functions to perform secret message embedding and allied pixel adjustment (optimization). This approach leads to better image quality, visual imperceptibility and higher embedding capacity even without losing original quality. These all features make the proposed system suitable for numerous communication purposes including cloud communication, healthcare data communication, IoT communication purposes etc. MATLAB based model development and its simulation with different datasets as well as secret text of varied sizes revealed that the proposed model could be attack resilient (statistical assessment based attack models) and quality-centric (high PSNR) which make it suitable for secure medical data transmission over cloud platforms.

Acknowledgements The authors like to express their great appreciation to Mr. M. Santhoshkumar for his valuable and constructive suggestions during this research work's planning and development. His willingness to give his time so generously has been very much appreciated. The authors also would like to thank the anonymous reviewers for their insightful suggestions and careful reading of the manuscript.

References

1. Abd-El-Atty B, Iliyasu AM, Alaskar H, Abd El-Latif AA (2020) A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors. 20(11):3108
2. Ahmad S, Thanikaiselvan V, Amitharajan R (2017) Data security through data hiding in images: a review. J Artif Intell 10:1–21
3. Ahmad M, Doja M, Sufyan Beg M (2018) Security analysis and enhancements of an image cryptosystem based on hyperchaotic system, J. King Saud Univ Comput Inf Sci:1–9
4. Ahmed DEM, Khalifa OO Robust and Secure Image Steganography Based on Elliptic Curve Cryptography, vol 2014. 2014 International conference on computer and communication engineering, Kuala Lumpur, pp 288–291. https://doi.org/10.1109/ICCCE.2014.88
5. Alam MS (2017) Secure M-commerce data using post quantum cryptography. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, pp 649–654. https://doi.org/10.1109/ICPCSI.2017.8391793
6. Al-barazanchi I, Shawkat S, Hameed M, Al-badri K (2019) Modified RSA-based algorithm: a double secure approach. Telkomnika Indonesian J Electric Eng 17:2818–2825. https://doi.org/10.12928/TELKOMNIKA.v17i6.13201
7. Anwar A, A.Ghany K, Elmahdy H (2015) Improving the security of images transmission. Int J Bio-Med Informat e-Health 3:7–13
8. B. PUSHPA (2020) Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth international conference on computing methodologies and communication (ICCMC), Erode, India, pp. 329–334, DOI: https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00062.
9. Anupam Kumar Bairagi, Rahmatullah Khondoker, and Rafiqul Islam. 2016. An efficient steganographic approach for protecting communication in the Internet of Things IoT critical infrastructures. Inf. Sec. J.: A Global Perspective 25, 4–6 (2016), 197–212. DOI: https://doi.org/10.1080/19393555.2016.1206640
10. Bashir Abugharsa A, Basari AS, Almangush H (2012) A New Image Encryption Approach using the Integration of a Shifting Technique and the AES Algorithm. Int J Comput Appl 42:36–45. https://doi.org/10.5120/5723-7785
11. Chidambaram N, Raj P, Thenmozhi K, Rajagopalan S, Amirtharajan R (2019) A cloud compatible DNA coded security solution for multimedia file sharing & storage. Multimed Tools Appl 78:33837–33863. https://doi.org/10.1007/s11042-019-08166-z
12. Duluta A, Mocanu S, Pietraru R, Merezeanu D, Saru D (2017) Secure Communication Method Based on Encryption and Steganography. 2017 21st international conference on control systems and computer science (CSCS), Bucharest, pp 453–458. https://doi.org/10.1109/CSCS.2017.70
13. El-Emam NN, Al-Diabat M (2015) A novel algorithm for colour image steganography using a new intelligent technique based on three phases. Appl Soft Comput 37:830–846
14. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608
15. Gupta K, Silakari S (2012) Novel approach for fast compressed hybrid color image cryptosystem. Adv Eng Softw 49:29–42
16. Gupta RK, Singh P (2013) A new way to design and implementation of hybrid crypto system for security of the information in public network. Int J Emerg Technol Adv Eng 3(8):108–115
17. Hajduk V, Broda M, Kovac O, Levicky D (2016) Image steganography with using QR code and cryptography. 2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA), Kosice, pp 350–353. https://doi.org/10.1109/RADIOELEK.2016.7477370
18. Hashim MM, Taha MS, Aman AHM, Hashim AHA, Rahim MSM, Islam S Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography, vol 2019. 2019 7th international conference on mechatronics engineering (ICOM), Putrajaya, pp 1–6. https://doi.org/10.1109/ICOM47790.2019.8952061
19. Input images available URL (2021), "htttps://homepages.cae.wisc.edu/~ece533/images/".
20. Jain M, Choudhary RC, Kumar A (2016) Secure medical image steganography with RSA cryptography using decision tree. 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, pp 291–295. https://doi.org/10.1109/IC3I.2016.7917977
21. Kadhim KT, Alsahlany AM, Wadi SM, Kadhum HT (2020) An overview of Patient's health status monitoring system based on internet of things (IoT). Wireless Pers Commun 114:2235–2262. https://doi.org/10.1007/s11277-020-07474-0
22. Khalil MI (2017) Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. Int J Comput Network Inform Secur 9:22–28. https://doi.org/10.5815/ijcnis.2017.02.03

23. Kumar N, Agrawal S (2014) An efficient and effective lossless symmetric key cryptography algorithm for an image. 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, pp 1–5. https://doi.org/10.1109/ICAETR.2014.7012788
24. Laskar S (2012) High capacity data hiding using LSB steganography and encryption. Int J Database Manag Syst 4:57–68. https://doi.org/10.5121/ijdms.2012.4605
25. Leung Y, Hou RY (2015) Unequal security protection for secure multimedia communication. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, pp 570–571. https://doi.org/10.1109/GCCE.2015.7398667
26. Li L, Hossain MS, El-Latif AAA et al (2019) Distortion less secret image sharing scheme for internet of things system. Cluster Comput 22:2293–2307. https://doi.org/10.1007/s10586-017-1345-y
27. Liao X, Yin J, Guo S, Li X, Sangaiah AK (2018) Medical JPEG image steganography based on preserving inter-block dependencies. Comput Electri Eng 67:320–329, ISSN 0045-7906. https://doi.org/10.1016/j.compeleceng.2017.08.020
28. Madhusudhan KN, Sakthivel P (2020) A secure medical image transmission algorithm based on binary bits and Arnold map. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02028-5
29. Mansour RF, Abdelrahim EM (2019) An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. Multidim Syst Sign Process 30:791–814. https://doi.org/10.1007/s11045-018-0575-3
30. Mare SF, Vladutiu M, Prodan L (2011) Secret data communication system using steganography, AES and RSA. 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), Timisoara, pp 339–344. https://doi.org/10.1109/SIITME.2011.6102748
31. Masood I, Wang Y, Daud A, Aljohani NR, Dawood H (2018) Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure. Wireless Commun Mobile Comput 2018(2143897): 23. https://doi.org/10.1155/2018/2143897
32. May Zaw, Z., and S. W. Phyo. “Security Enhancement System Based on the Integration of Cryptography and Steganography”. Int J Comput (IJC), Vol. 19, no. 1, Oct. 2015, pp. 26–39.
33. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2018) Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Future Gener Comput Syst 86:951–960
34. Mukhedkar M, Powar P, Gaikwad P (2015) Secure non real time image encryption algorithm development using cryptography & steganography. 2015 Annual IEEE India Conference (INDICON), New Delhi, pp 1–6. https://doi.org/10.1109/INDICON.2015.7443808
35. Nithyabharathi PV, Kowsalya T, Baskar V (2014) To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES. IJSETR 3(2)
36. Ou B, Li X, Zhao Y, Ni R (2015) Efficient color image reversible data hiding based on channel dependent payload partition and adaptive embedding. Signal Process 108:642–657. https://doi.org/10.1016/j.sigpro.2014.10.012
37. Panchal D (2015) An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing. IJEDR 3(4) ISSN: 2321-9939
38. Pandey HM (2020) Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Future Gener Comput Syst 111:213–225, ISSN 0167-739X. https://doi.org/10.1016/j.future.2020.04.034
39. Parah SA, Sheikh JA, Ahad F, Bhat GM (2018) High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems. In: Dey N, Hassanien A, Bhatt C, Ashour A, Satapathy S (eds) Internet of things and big data analytics toward next-generation intelligence. Studies in big data, vol 30. Springer, Cham. https://doi.org/10.1007/978-3-319-60435-0_17
40. Paschou M, Sakkopoulos E, Sourla E, Tsakalidis A (2013) Health internet of things: metrics and methods for efficient data transfer. Simulation Modelling Practice and Theory 34:186–199, ISSN 1569-190X. https://doi.org/10.1016/j.simpat.2012.08.002
41. Patil P, Narayankar P, Narayan DG, Meena SM (2016) A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comput Sci 78:617–624, ISSN 1877-0509. https://doi.org/10.1016/j.procs.2016.02.108
42. RajeshKumar N, Yuvaraj D, Manikandan G, Balakrishnan R, Karthikeyan B et al (2020) Secret image communication scheme based on visual cryptography and tetrolet tiling patterns. Comput Mater Continua 65(2):1283–1301
43. Ramalingam B, Rengarajan A, Rayappan JBB (2017) Hybrid Image Crypto System for Secure Image Communication- A VLSI Approach. Microprocess Microsyst. https://doi.org/10.1016/j.micpro.2017.02.003

44. Rathore S, Sharma PK, Loia V, Jeong Y-S, Park JH (2017) Social network security: Issues, challenges, threats, and solutions, Information Sciences, vol 421, pp 43–69, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2017.08.063.
45. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R (2017) DNA Chaos blend to secure medical privacy. IEEE Trans NanoBiosci 16(8):850–858. https://doi.org/10.1109/TNB.2017.2780881
46. Razzaq MA, Shaikh RA, Baig MA, Memon AA (2017) Digital image security: Fusion of encryption steganography and watermarking, Int. J Adv Comput Sci Appl 8(5):224–228
47. Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo SS, Mehmood I (2017) Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimed Tools Appl 76:3519–3536. https://doi.org/10.1007/s11042-016-3811-6
48. Sajjad M, Nasir M, Muhammad K, Khan S, Jan Z, Sangaiah AK, Elhoseny M, Baik SW (2020) Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. Future Gener Comput Syst 108:995–1007, ISSN 0167-739X. https://doi.org/10.1016/j.future.2017.11.013
49. Saleh ME, Aly AA, Omara FA (2016) Data security using cryptography and steganography techniques. Int J Adv Comput Sci Appl (IJACSA) 7(6). https://doi.org/10.14569/IJACSA.2016.070651
50. Setyaningsih E, Wardoyo R, Sari AK (2020) Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution. Digital Commun Networks, ISSN 2352-8648. https://doi.org/10.1016/j.dcan.2020.02.001
51. Seyedzadeh SM, Mirzakuchaki S (2012) A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal Process 92(5):1202–1215
52. Shahzadi S, Iqbal M, Dagiuklas T, Qayyum ZU (2017) Multi-access edge computing: open issues, challenges and future perspectives. J Cloud Comput 6. https://doi.org/10.1186/s13677-017-0097-9
53. Shankar K, Lakshmanaprabu SK, Gupta D, Khanna A, de Albuquerque VHC (2020) Adaptive optimal multi key-based encryption for digital image security. Concurrency Computat Pract Exper 32:e5122. https://doi.org/10.1002/cpe.5122
54. Shilpi Harnal RK Chauhan (2019) Hybrid Cryptography based E2EE for Integrity &Confidentiality in Multimedia Cloud Computing. IJITEE 10(8)
55. Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. J Network Comput Appl 79: 88–115, ISSN 1084-8045. https://doi.org/10.1016/j.jnca.2016.11.027
56. Sivaswamy J, Krishnadas SR, Joshi GD, Jain M, Ujjwaft Syed Tabish A (2015) Drishti-GS: Retinal image dataset for optic nerve head (ONH) segmentation. 2014 IEEE 11th International Symposium on Biomedical Imaging, ISBI 2014. pp. 53–56. https://doi.org/10.1109/ISBI.2014.6867807
57. Sreekutty MS, Baiju PS (2017, pp. 1-5) "security enhancement in image steganography for medical integrity verification system," 2017 international conference on circuit. Kollam, Power and Computing Technologies (ICCPCT). https://doi.org/10.1109/ICCPCT.2017.8074197
58. Stoyanov B, Stoyanov B (2020) BOOST: medical image steganography using nuclear spin generator. Entropy. 22(5):501
59. Su N, Zhang Y, Li M (2019) Research on Data Encryption Standard Based on AES Algorithm in Internet of Things Environment. 2019 IEEE 3rd information technology, networking, electronic and automation control conference (ITNEC), Chengdu, pp 2071–2075. https://doi.org/10.1109/ITNEC.2019.8729488
60. Usman MA, Usman MR (2018) Using image steganography for providing enhanced medical data security. 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, pp 1–4. https://doi.org/10.1109/CCNC.2018.8319263
61. Venkatraman K, Geetha K (2019) Dynamic virtual cluster cloud security using hybrid steganographic image authentication algorithm. Automatika 60(3):314–321. https://doi.org/10.1080/00051144.2019.1624409
62. Wajgade VM (2013) Enhancing Data Security Using Video Steganography. Int J Emerg Technol Adv Eng 3(4)
63. Y. Wu, J. P. Noonan, S. Agaian, “NPCR and UACI randomness tests for image encryption”, Cyber J: Multidis J Sci Technol, J Select Areas Telecommun (JSAT), April Edition, 2011, pp.31–38, 2011.
64. Yaghouti Niyat A, Moattar MH, Niazi Torshiz M (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optic Laser Eng 90:225–237
65. Rupeng Yang, Qiuliang Xu, Man Ho Au, Zuoxia Yu, Hao Wang, Lu Zhou, Position based cryptography with location privacy: a step for fog computing, Future Gener Comput Syst, volume 78, Part 2, 2018, Pages 799–806, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.05.035.
66. Yu L, Wang Z, Wang W (2012) The Application of Hybrid Encryption Algorithm in Software Security. 2012 Fourth international conference on computational intelligence and communication networks, Mathura, pp 762–765. https://doi.org/10.1109/CICN.2012.195

67. Yu J, Li H, Liu D (2020) Modified Immune Evolutionary Algorithm for Medical Data Clustering and Feature Extraction under Cloud Computing Environment. J Healthcare Eng 2020(1051394):11. https://doi.org/10.1155/2020/1051394
68. Zhang M, Tong X-J (2015) A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system. Multimed Tool Appl 74(24):1125–11279

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

Affiliations

R. Denis [1] **· P. Madhubala** [2]

P. Madhubala
madhubalasivaji@gmail.com

[1] Department of Computer Science, Periyar University, Salem, TN, India

[2] Department of Computer Science, Don Bosco College (Affiliated to Periyar University), Dharmapuri, TN, India