RESEARCH ARTICLE

Evolutionary Computing Assisted Visually-Imperceptible Hybrid Cryptography and Steganography Model for Secure Data Communication over Cloud Environment

Denis R
Department of Computer Science, Periyar University, Salem, Tamil Nadu, India
denisatshc@gmail.com

Madhubala P
PG & Research Department of Computer Science, Don Bosco College, Dharmapuri, Tamil Nadu, India
madhubalasivaji@gmail.com

Published online: 25 December 2020

Abstract – The exponential growth of communication technologies and related application environments has broadened the cloud computing ecosystem horizon to meet major communication needs. However, in-parallel upsurge in online attacks, security breaches or allied intrusion events has alarmed industries to ensure optimal data security. Unlike text data transmission, image, or other multimedia communication over the cloud requires computational efficiency, imperceptibility, etc. to meet attack-resilient transmission. Amongst the major available security systems, the combination of cryptosystems and steganography has been identified as an augmented security model for data transmission. However, it demands enhancement in both stages to meet cloud-specific communication efficiency. Considering it as motivation, in this paper an efficient Visually Imperceptible Hybrid Crypto-Steganography (VIHCS) model is developed using Hybrid Cryptosystems followed by Adaptive Genetic Algorithm assisted Least Significant Bit (LSB) embedding process. We developed a novel Hybrid Cryptosystem by strategically applying Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to secure secret data to be embedded in a cover image. In addition, the use of the Adaptive Genetic Algorithm based Optimal Pixel Adjustment (AGA-OPAP) strengthened the Least Significant Bit embedding while retaining the best possible image quality and visual imperceptibility. The proposed model achieved higher security, high embedding capacity as well as image quality, which is vital for cloud communication. To perform LSB embedding we applied 2D-Discrete Wavelet Transform (2D-DWT-2L) method with 8×8 dimensional block-wise embedding. It helps to achieve better embedding efficiency in conjunction with the AGA-OPAP model. Simulation results and respective visio-statistical assessment revealed that the proposed VIHCS model can accomplish better performance and reliable secure data communication over the cloud environment. Thus, the VIHCS model achieves maximum possible imperceptibility and hence can avoid attacks- such as steganalysis based attack or RS-attacks.

Index Terms – Secure Data Transmission, Cloud Environment, Hybrid Cryptography-Steganography Model, Evolutionary Computing, Encryption and Decryption, Adaptive Genetic Algorithm (AGA), Least Significant Bit (LSB).

1. INTRODUCTION

The exponential growth of software and advanced hardware systems has expanded the scope to fully integrated services and solutions that meet diverse socio-industrial demands. Data communication and allied forces of the exchange of knowledge have gained broad popularity around the world among the largest emerging applications. On the other hand, high speed development in internet technology and related applications has resulted in different innovations such as cloud computing, Internet-of-Things (IoT), etc. However, ensuring secure communication across these application environments has always been a challenge for industries [1-8]. Various uses, including social networking sites, medical services industry, e-commerce, scientific societies, the financial sector, other industrial needs, such as monitoring and security systems, etc have been met daily by vast numbers of communication systems enabling the Internet.

Social networking and entertainment, tracking footages [3, 4, 5], user data and an IoT communications support environment [2], [4], [6-12] all have to be secured from unauthorized access to their data by protection measures and policies. Undeniably, corporate software has also seen a substantial increase in vast volumes of data generation and collaboration through the industry, government departments, banks, and other organizations. In practice, such data are used for certain targeted analysis or observation to make a suitable decision.

Cloud computing has been created through the amalgamation of the various data sources and the combination of a large volume of data. Cloud computing refers to "free access to shared, configurable computing resources and applications that can be used for a price through telecommunications (such as the Internet) on request". There are three main forms of cloud computing generally known as:

- IaaS – Infrastructure as a Service
- PaaS – Platform as a Service
- SaaS – Software as a Service.

XaaS is a term that refers to the provision of anything as a service. It recognizes the vast number of goods, software, and technology currently offered by suppliers to consumers as a service across a network, not locally or on-site in a sector. Few examples for XaaS include Storage as a Service, Database as a Service, Security as a Service, Malware as a Service, Distributed Denial of Services, Disaster Recovery as a Service, Communications as a Service and the Network as a Service, and so on.

One of the key features of cloud computing is that it provides a range of stakeholders with access to data, real-time computing, and cloud-based decisions, regardless of origin or geographical barriers. However, information exchange from one node or user to another or across the cloud platform is highly vulnerable until a robust security measure is not provided. One of the predominant concerns in cloud computing is the protection or seamless exchange of private data, particularly multimedia (video, audio, image) [1 - 4].

In addition to secure communication, enabling computational efficacy is also a must, as it (i.e., cloud computing) demands time-efficient and reliable computation to meet the application's real-time requirements. It signifies the assurance of security, scalability, and manageability in the cloud computing environment for up-surging computational and allied communication demands. Facilitating security of the data has become inevitable for cloud environments like social media, the healthcare sector, etc [3][4][6][9-11]. There are major threats to the complex design of cloud implementations with vision and control loss. The continuous change in the security perimeter due to the elastic boundary of cloud use also calls for a more complex security approach.

During data communication, once a miscreant gets data access or retrieves the data or allied content, it can easily modified or misused for a certain targeted or intended goal. To avoid such incidents, various attempts have been made to incorporate protection systems; however, substantial efforts are being made either by integrating security models for data access or security of infrastructure or by introducing such on-data security features [12]. In other words, researchers have created protective models in which the user has to be authenticated or the data itself is protected before accessing the data (access-control) to prevent the unauthorized access or intruder from revealing sensitive data.

Several attempts have been made over the past few years to strengthen data protection in the cloud computing world. However, ensuring both levels of security and computational efficiency has remained an open research area for academia-industries. Amongst the major data security models, steganography and cryptosystems have played a decisive role; however, in practice, these methods as a standalone solution have been found limited due to parallel increase in attacking models. This paved way to design Hybrid Cryptography-Steganography which has gained widespread attention [9-12], where the dual-level of security enables or provides better data security. However, as an application-specific scenario, retaining secure and attack resilient data transmission demands enhanced steganography as well as cryptosystem to accomplish the above stated eventual goal. Realizing the data communication over cloud infrastructure which is becoming vulnerable these days due to increased attacking efforts, in this paper the focus is made on enhancing both steganography as well as cryptosystems.

To achieve it, at first, a Hybrid Cryptosystem is designed using RSA and AES cryptography algorithms. In the proposed model these cryptography algorithms are applied in a strategic manner that ensures an enhancement in security level. The hybrid cryptosystem proposed is used to encrypt the secret text data which is embedded into the cover image. Once performing secret text encryption, an Evolutionary Computing (EC) assisted LSB embedding model is applied 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, the AGA algorithm was applied to perform Optimal Pixel Adjustment Process (OPAP) during LSB embedding. The use of AGA-OPAP based LSB embedding has achieved an optimum Peak Signal to Noise Ratio (PSNR) with negligible histogram pattern variance and RS parameters, rendering the overall process quality-centric and Visio-imperceptible. Such novelties can help the proposed model avoid attacks like Steganalysis or RS attacks which are well known for their ability to exploit statistical variations in image data to detect secret or hidden information. The overall proposed model is developed using the MATLAB tool 2018a. The proposed security method achieves enhanced or augmented security for data communication over the cloud environment.

The remaining parts of the manuscript are as follows: Section 2 addresses related work, followed by section 3 research objectives and section 4 problem formulation. Section 5 discusses the proposed system model, while the findings obtained and their respective inferences are discussed in Section 6. Section 7 ends with the conclusion.

2. RELATED WORK

This research intends to propose a secure data communication model for a cloud computing environment for which amalgamating enhanced steganography and cryptosystem can be of utmost significance. With this motive, in this section, a few key literatures on these techniques are discussed with their respective strengths as well as limitations.

Xue et al [13] suggested adaptive steganography based on "Sum and Difference Covering Set" (SDCS) information, where the noisiest pixels are initially detected according to an iterative noise-level estimation model. The secret hidden data is then entrenched using the SDCS algorithm into these noisy pixels. However, this approach could not employ any additional layer of security to strengthen overall efficacy.

Vipula et al [14] merged crypto-algorithm AES with steganography to conceal secret text data in multimedia files. But the main issues of signal strength and imperceptibility, which are necessary for modern-day applications are not addressed.

Saleh et al [15] recommended the modified AES algorithm to encrypt a secret message, which was then processed for hiding in the cover image [16]. However, Duluta et al.[17] recently found that some traditional models for encryption have a range of limitations that can restrict their cloud computing environment suitability. Authors focused only on image type of data; though it needs further verification for computational efficacy and performance trade-off under different test conditions.

Pancha et al [18] applied a cryptosystem with steganography for safe data communication. First, the authors used encryption, in combination with the chirikov mapping, to turn the input image into a cipher image. Then authors used steganography to hide the encrypted image from the cover image during the sequential process. However, it did not discuss the enforced cases of entropy and histogram distortion.

Leung et al.[19] proposed uneven security protection by using multiple encryption technologies to secure various media pieces of different importance. Their model focuses primarily on augmenting only the cryptosystem and therefore needs further enhancement of signal retention in steganography.

Towards video fingerprinting, Li et al [20] applied the theory of recognition and clustering of the field of interest. However such approaches cannot be the optimal solution to meet the current high-speed real-time communication requirements, especially over cloud infrastructure.

Ahmed et al [21] presented a model based on a user interface in which the sender could pick the appropriate cover and secret message that was processed using Elliptic Curve Cryptography based encryption trailed with LSB embedding. The processed data were transmitted to the same target through different channels. However, efforts can be made to improve their model for lightweight encryption and attack resilient embedding.

To achieve a better solution and high non-perceptibility, Hajduk et al [22] proposed a technique of image steganography where the text message was encrypted and inserted in the cover image using the Quick Response Code (QRC). Besides that, the suitability for multimedia data communication in a cloud environment has not been addressed.

Mukhedkar et al [23] has applied various cryptosystems to encrypt secret data before embedding it in the cover image for efficient and reliable multimedia transmission. The main emphasis was on cryptosystem enhancement and other aspects of real-time multimedia transmission were not discussed.

Unlike traditional cryptosystems, Alam et al [24] used McElice's cryptosystem to encrypt or decrypt data to improve data protection across wireless networks. Their method could not be used for cloud communication with massive databases containing multimedia content. Depicting limitations of classical cryptosystems, Kumar et al [25] proposed a public key cryptographic algorithm for safe 3D color data communication.

Gupta et al [26] suggested the use of Discrete Wavelet Transform, given the fact that better multimedia data processing techniques such as wavelet analysis will help in increase the imperceptibility of hidden data over uncertain channels. DWT was applied to split the input image into four sub-bands, followed by hiding data within the splits. The image was compressed before transmission after hiding the secret text information. The authors [26][27] implemented a new hidden data communication method using RSA and AES in conjunction with steganography. However for cloud-based environments where QoS/QoE is of critical importance, splitting data into several chunks and embedding data, further decompression and/or decryption of original data elements may be too cumbersome and voluminous in computation.

Anwar et al [28] suggested a combination of algorithms to improve the protection of medical images during transmission in uncertain channels. Liao et al [29] developed a medical JPEG image steganographic scheme aimed at maintaining inter-block DCT coefficient dependences. Both the approaches exhibit good results in image quality but the security of the data still needs enhancement.

Using blended chaotic maps and Haar Integer Wavelet Transform (HIWT), Balakrishnan et al [30] suggested a transform domain hybrid image cryptosystem. It can be improved by efficient key generation, substitution-permutation, uncertainty, and diffusion processes.

Based on deoxyribonucleic acid and several chaotic maps, a hybrid encryption algorithm was projected to encrypt DICOM color images by Divya et al [31]. It requires a better concept of embedding with minimal noise probability and lightweight cloud computing encryption.

To ensure optimal communication over volatile networks, Mansour et al [32] suggested the Discrete Ripplet Transformation technique for embedding messages in medical cover images. This model focuses on embedding and can be further improved to be attack-resilient with hybrid cryptosystems and effective wavelets.

Usman et al [33] employed Swapped Huffman tree encoding to provide multiple encryptions for medical data. It still has computational overheads, however, and is likely to be attacked by advanced steganalysis/attacks.

To secure medical data, Hashim et al [34] suggested a new steganography mechanism based on the Bit Invert Method (BIS) using three random control parameters. It can be further improved by implementing the required embedding principle to prevent all types of attacks.

Nithya et al [35] have developed an integrated security system using DNA coding and image encryption methods to provide enhanced security. This strategy has shown good results but does not solve data redundancy.

Harnal et al [36] proposed an end-to-end cryptography (E2EE) hybrid cryptography algorithm to maintain integrity and confidentiality in a multimedia cloud computing environment. This mechanism was easy and deals with limited database sizes.

Using a nuclear spin generator, Stoyanov et al [37] implemented a medical image stego hiding approach and examined the findings based on histogram analysis and peak signal-to-noise ratio. However, there is significant potential to enhance the authentication mechanism for the cloud computing environment.

A robust, quasi-quantum walk-based image steganography mechanism has been developed by Baseem et al [38] to support secure transmission on the cloud-based E-healthcare platform. The scheme has achieved good visual quality, resistance to data loss attacks, high embedding capability, and robust protection. It can be improved by applying an effective bio-inspired optimization technique to attain even better performance.

Madhusudhan et al [39] have implemented a secure multimedia transmission algorithm based on binary bits and a map of Arnold. The idea of hiding data can be implemented to improve security.

Emy et al [40] proposed a viable method for transmitting color images using a compression-encryption model with a dynamic key generator and robust symmetric key distribution. Pandey et al [41] developed a bit mask-oriented genetic algorithm based on a resilient data transmission mechanism. Encrypted data was embedded in medical images through Discrete Wavelet Transformation at 1 and 2 levels (DWT). Protection can be further improved with a hybrid cryptosystem so that there is no possibility of any cryptanalysis/attacks.

This is a matter of fact that a range of research has been done to perform data embedding in images/medical image using steganography techniques, but most of the methodologies use wavelet transformation techniques and focus on either PSNR enhancement or capability enhancement embedding. The requirements such as Region of Interest preservation, maximum imperceptibility, small or negligible histogram variations, resistance to statistical attacks, higher PSNR, low entropy, MAE, Correlation analysis etc. were in need to be enhanced for better performance.

Literature also reveals that in the field of image encryption and cryptography techniques, only few have used metaheuristic algorithms. In some recent studies, evolutionary algorithms have been successfully applied to overcome the issue of safe data communication. It is vital to build a computationally equipped algorithm based on the discussion thus far, that not only provides security while data transmission but also addresses broad search regions.

The work carried out to date provides security and privacy, but mostly suffers from some barriers, such as managing wide search spaces, avoiding duplication, etc. Therefore by developing a fusion of cryptography theory and steganography with adaptive genetic algorithm-based RS attack, we propose an effective algorithm to resolve these limitations by resilient embedding-based secure data transmission over the cloud environment.

3. RESEARCH OBJECTIVES

- To propose a Hybrid Crypto-Steganography Model for effective secure data communication over the cloud environment.
- To implement a Hybrid Cryptosystem to secure text data to be embedded in the cover image.

- To apply the Genetic Algorithm (GA) principle to the Optimal Pixel Adjustment Process to preserve maximum possible data embedding capability, maximum imperceptibility, and higher PSNR for reliable cloud-based data communication.
- To test the simulation analysis and the performance of the proposed model against the existing approaches.
- To prove the Adaptive Genetic Algorithm based OPAP assisted LSB embedding with Hybrid Cryptosystem accomplish an optimal solution for secure data communication over the cloud environment.

4. PROBLEM FORMULATION

As already stated, the exponential rise in Cloud assisted IoTs also called Cloud-IoT has also alarmed scientific society to develop QoS centric (image) transmission systems. Unlike conventional research so far where the emphasis is merely on increasing efficiency and timely delivery, there is an unavoidable need to build a more effective and robust safe transmission system. Several attempts have been made, such as cryptosystems, steganography, etc., considering the inevitable significance of secure communication, particularly for the Cloud-IoT environment. Taking Cryptosystem as a potential solution, two types of symmetric and asymmetric crypto algorithms are still subject to major limitations, such as computation overheads, time, and the probability of security breaches that have occurred globally in recent years. Strategies such as Brute-Force attacks, MySql attacks, and many other well-known methods of attack often carry data security under suspicious circumstances.

Considering the contemporary application environment, where users use internet technologies, cloud infrastructures, or wireless communication media to transmit data from one peer to another, the risk of attack becomes more severe. In the last few years, the cases of unauthorized multimedia content access, image manipulation, personal multimedia file access, and publication, etc. have increased significantly. Towards multimedia data, especially image data security two techniques named steganography and cryptography have gained widespread attention. However, the steganography concept has broader significance towards multimedia data security over the cloud environment.

Steganography uses the principle of signal destruction by increasing entropy to the cover image or the division and transmission of content across various channels to the receiver. This mechanism allows data protection and reliability even after the intruder or miscreants have access to the data through the use of modern attacker modules or intrusion efforts. Considering the classical methods of steganography, it can be found that such methods cannot guarantee optimum efficiency due to increased entropy in the original image which makes data communication suspicious. On the other hand, splitting image data into multiple parts and transmitting it to the receiver through different channels to avoid unauthorized attacker access to data can impose huge computational costs, delays, resource exhaustion, etc., which cannot be used for a present cloud environment.

Considering the contemporary shortcomings of both cryptosystems, such as classical RSA, Elliptic Curve Cryptography (ECC), AES, etc, and steganography, using these methods together can be of critical importance. Such hybrid security models can provide a dual level of security where steganography can assist in hiding significant details in cover data, while cryptography can ensure that the intruder could not access the data hidden without authorizing credentials. Exploring in-depth, it can be found that introducing Hybrid Crypto-Steganography (HCS) concept can help to achieve a more efficient outcome, however at the increased computational overheads. This is because in major conventional approaches, to increase security prospects authors have applied a high bit size cryptosystem; however, it functions at the cost of increased computational complexities at both transmitter as well as receiver side. It reduces the efficacy of the HCS systems. On contrary, embedding data inside a cover image to ensure its security depends on the method or efficacy of the steganography, as with a less effective approach embedding higher data might expose data to get noticed by an intruder. Moreover, embedding excessive or inappropriate data to the cover image might reduce or degrade data quality at the receiver and hence can affect overall communication efficiency. In such cases, enabling optimal trade-off between computational efficiency as well as data quality is vital for HCS.

Considering it as motivation, in this research paper, the focus is made on developing a robust and computationally efficient HCS model for a cloud computing environment. Undeniably, HCS systems encompass both cryptography and steganography as computing models; however, the classical cryptosystems such as RSA, ECC, AES, etc are computationally costly, especially when the level of security has to be achieved higher. In other words, a 64 bit RSA or AES would have relatively lower coefficients for data encryption [4-5][42-43]; on contrary increasing bit size often results in amplified computational overheads. However, on the other side, the efficacy of ECC cryptosystem's too decisively depends on the selection of curve points or the allied parameter selection, which turns out to be a computationally complex task. On contrary, cloud computing and allied data transmission require a time and computation efficient environment.

In this research we have designed a Hybrid Cryptosystem model by strategically implementing AES and RSA cryptography algorithms to secure secret data to be embedded with a cover image. In the HCS system, the second and most critical function is steganography too requires efficient data decomposition, data embedding, and further data reconstruction. In major conventional researches authors have merely focused on either achieving higher PSNR or embedding capacity; however, maintaining an optimal balance between these two has always been a trivial task. On the other hand, data communication over cloud infrastructure requires optimal data quality, higher transmission rate as well as more time-efficient computation. However, there is numerous cloud-based application environment where maintaining an optimal quality of the multimedia data is a must. In major conventional efforts where authors have tried to embed more data in the cover have undergone an increased level of entropy and resulting degradation in data quality. Such approaches can't be suitable for applications such as telemedicine, critical multimedia image transmission, etc. The inclusion of entropy and its visual reveal might help intruders attacking that specific data under communication. In such cases maintaining optimal data embedding with low entropy and maximum possible data quality can be vital.

To achieve it, enhancement in data (say, image) decomposition, strategically optimized data embedding, and highly efficient pixel adjustment followed by data reconstruction is a must. Exploring in-depth, it can be found that optimizing pixel adjustment when embedding data within the cover image can be of great significance to enhance both embedding capacity as well as PSNR. Considering it as a motive, in this research an Evolutionary Computing concept-based OPAP model is developed that intends to achieve optimal LSB embedding with optimal adaptive pixel adjustment. Specifically, in this paper Multi-Objective Optimization (MOO) centric GA algorithm has been developed which intends to optimize both PSNR as well as regular and singular coefficients of each image block simultaneously (to ensure quality as well as visual imperceptibility).

The proposed AGA-OPAP model dynamically adjusts pixels of the cover images to retain optimal PSNR, low entropy with maximum possible data embedding capacity. Noticeably, in the steganography model, DWT is often used to facilitate image decomposition with 8×8 window size and performs 8 bit LSB embedding, which has been further optimized using AGA-OPAP. Thus, the proposed model achieves more secure, high-capacity, and attack-resilient steganography to perform data communication over cloud infrastructure. Thus, the proposed HCS backed AGA-OPAP based LSB embedding model and resulting Visio-Imperceptible-HCS (VIHCS) model can achieve an optimally secure and computationally efficient data communication paradigm for cloud environment. The proposed VIHCS model can effectively alleviate the possibilities of low pass filtering, Regular and Singular (steganalysis) RS attack, Brute-Force etc. type of attack scenarios.

5. PROPOSED SYSTEM MODEL

This section discusses the proposed VIHCS model and allied implementation. The Figure 1 depicts the process flow of the proposed model.

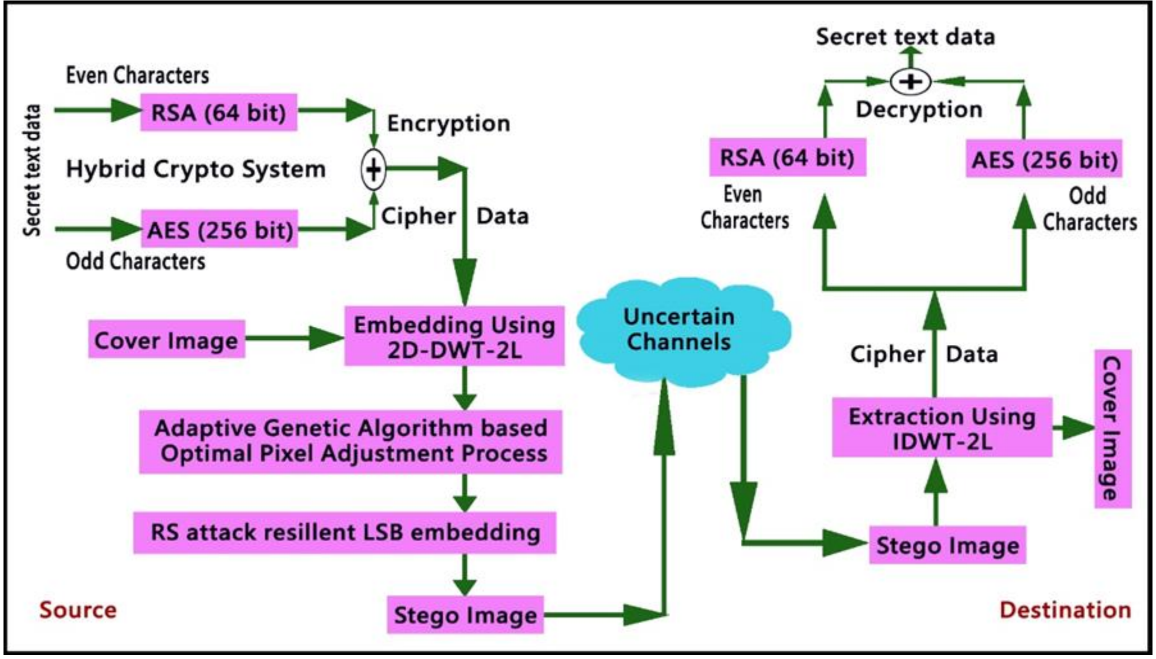


Figure 1 The Proposed VIHCS Model for Secure Data Communication

5.1. Data Encryption

There are numerous cloud-assisted application environments in which different data, including image and text, are transmitted under uncertain channel conditions. Some of the common applications are telemedicine in the healthcare sector, social media, etc. Such applications can even have composite data as the amalgamation of text as well as an image (for example, in telemedicine both patients scanning medical reports as well as 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 multilevel security can have augmented strength to alleviate any breach of security or unauthorized data access. Taking into account it as an objective, a novel hybrid cryptosystem is first developed in this research. 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. It embodies strategic implementation of both RSA and AES, which has been used to encrypt input text data which is at first converted into ciphertext to be embedded within the cover image.

The cryptographic model $\mathbb{C} = \{\mathrm{F}\eta, \mathrm{F}\eta^{-1}, C, S, T\}$ encompasses encryption and decryption processes. During the encryption process, at first, the 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 doesn't signify dividing content into two fractional parts, rather once converting the entire text into binary form, the overall bit sequence is processed in such a 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}, while RSA was used for T_{Even} encryption method same as [42]; however, we employed 256-bit AES, while the existing approach [42] considered 128-bit AES for encryption. Considering computational efficiency demands, we considered 64-bit RSA, while AES was applied as 256 bit. Though, RSA with low bit-size has often been criticized to have 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), and second, the consideration of low-bit size can avoid unwanted computation that eventually will make it robust to serve real-world applications. Additionally, AES-256 is almost six times faster and more efficient than classical triple-DES. Therefore, the inclusion of AES as a cryptographic method seems viable towards a robust 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 our proposed encryption model, AES-256 has 14 rounds of computation, while 64-bit RSA was applied as a single round itself, as it doesn't employ round-computation for confusion creation (to avoid side-channel attack). Though, with our proposed concept, AES-256 can be executed with lower rounds as well; however, will recommend more than 10 rounds to avoid detrimental consequences. 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 a 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, the inverse round transformation method applies four key functions, AddRoundKey, InvMixColumns, InvShiftRows, and InvSubBytes, sequentially. Due to the lack of space, the details of these key functions are not given in this manuscript. Thus, the overall process is mathematically modeled as follows:

$$C = \left\{E_{AES}, E_{RSA}, T_{odd}, T_{Even}, \hat{T}_{odd}, \hat{T}_{Even}, s, m, x\right\} \quad (1)$$

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

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

Input: Secret Text Input Data (S_{Text})

Output: Cipher Text, Key s

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 (see, [42])

Step-3 Encrypt S_{Text_odd} using AES-256 bit key size

$$Enc\_S_{Text\_odd} = AES - 256\left(S_{Text_{odd}}, s\right)$$

Step-4 Generate RSA keys (Public key m and private key x)

Step-5 Encrypt S_{Text_Even} using 64 bit-RSA

$$Enc\_S_{Text\_Even} = RSA - 64\left(S_{Text\_Even}, m\right)$$

```
Step-6 Construct combined Encrypted cipher data $Cipher\ _{F\_Total}$ by using both $Enc\_S_{Text\_odd}$ and $Enc\_S_{Text\_Even}$ in their indices
Step-7 $Enc_{Key} = AES(x, s)$ #$x$-round key, #s-secret key
Step-8 Create final cipher data $Cipher\ _{Tx}$
    $Cipher\ _{Tx} = Concatinate(Cipher\ _{F\_Total}, Enc_{Key})$
Step-9 Return $Cipher\ _{Tx}$ and $s$
End
```

Algorithm 1 Secret Data Encryption

Secret data encryption is shown in Algorithm 1. Once the text data has been encrypted it has been processed for Adaptive Genetic Algorithm based Optimal Pixel Adjustment Process assisted Least Significant Bit embedding. The detailed discussion of the proposed AGA-OPAP based LSB embedding model is given as follows:

5.2. AGA-OPAP Assisted LSB Embedding for VIHCS

5.2.1. DWT Analysis and LSB Embedding

To embed the critical information within the cover image to be transmitted over cloud infrastructure, at first it is important to decompose the input cover image and embed the cipher data optimally while ensuring minimum entropy, histogram variations, or PSNR reductions. To achieve this, we applied DWT because of its robustness and efficacy towards time as well as spatial domain analysis. In our proposed method, we applied a DWT with HAAR mother wavelet. We applied 2D-DWT-2L which was formulated as a sequential transformation process with the help of low pass and high pass filters towards the row of the image (blocks). To be noted, in the proposed 2D-DWT-2L concept, we considered level-2 coefficients to perform embedding, the key reason is it can provide a significant local feature set for text-embedding without impacting image quality significantly. Moreover, it can provide a more depth (feature) space for embedding, which as a cumulative solution with the proposed encryption can help to strengthen attack-resiliency and confusion.

Performing embedding with a single layer can cause higher visibility or perceptibility, and can also impact image quality post-embedding. On the other hand, embedding with a higher level coefficient can be more effective; however at the cost of increased computation, which can't be suitable for contemporary real-time application demands. Therefore, in this paper, we performed embedding with a 2-level DWT coefficient only. In this process, the results are discomposed towards the columns of the image. A snippet of this process is depicted through Figure 2 & Figure 3. The above-mentioned illustration (Figure 2 & Figure 3) depicts the elemental decomposition of the $C_j(N \times M)$, image of size N×M in the four distinct decomposed sub-bands (images), which are stated as high-high (HH), a high-low (HL), a low-high (LH), and a low-low (LL) frequency bands. Our proposed VIHCS model is designed to support visually imperceptible steganography to ensure maximum possible visual-imperceptibility that not only ensures seamless communication but also assists quality-data transmission, which is a must for cloud communication.

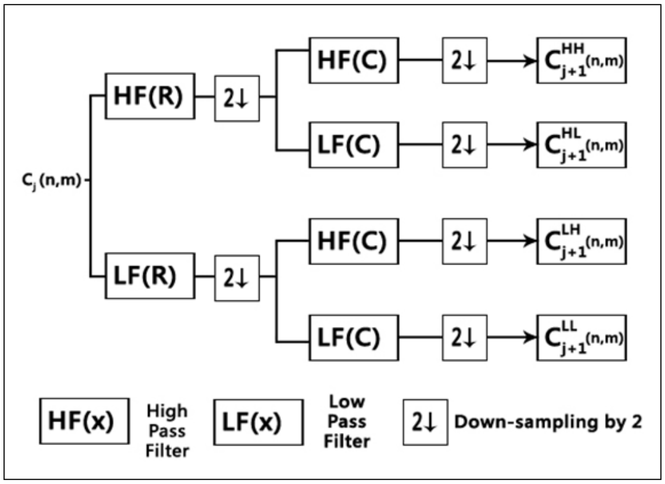


Figure 2 2D-DWT-2L Decomposition Process

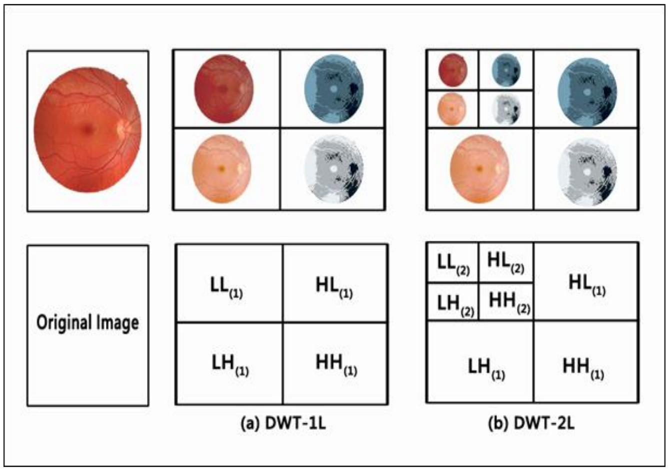


Figure 3 (a) DWT-1L (b) DWT-2L

To achieve it, we have designed VIHCS with $\widehat{S} = \{\{\mathrm{F}\eta, \mathrm{F}\eta^{-1}, C, S, T\}\}$. It comprises of three distinct methods including LSB embedding; AGA-OPAP assisted embedding optimization, and extraction processes. In the LSB embedding process, we consider a cover image C, the secret data T (which is already processed as cipher data ($Cipher\ _{Tx}$) is embedded using LSB embedding to produce stego image S.

Unlike classical efforts where authors have to embed text or cipher data arbitrarily or LSB without any optimization measure, in our proposed system, we have implemented an

EC assisted (say, heuristic model-based) pixel adjustment process. Our proposed system intends to ensure optimal pixel adjustment to retain maximum possible imperceptibility, quality preserve, and seamless transmission even under cloud attack conditions such as RS-Analysis or Steganalysis. In our proposed method, at first input image also called cover-image is processed using HAAR-DWT and the entire image is split into multiple blocks or 8×8 blocks. Considering literature and allied inferences towards the LSB embedding process, we have applied this approach to embed ciphertext in each block. Before discussing the process of AGA-OPAP assisted LSB embedding, a snippet of embedding mechanism is given as follows:

To perform embedding, at first cipher text is transformed into an ASCII format, which is then split into S_{Text_odd} and S_{Text_Even}. In this method, the odd values (i.e., S_{Text_odd}) are concealed in vertical coefficients as stated by LH2. Similarly, the even values are concealed in diagonal coefficients specified by high-level coefficients HH2.

The algorithm applied to perform embedding is given Algorithm 2.

```
Input: Cover Image
Output: Stego-Image
Step-1 Initiate the process
Step-2 Transform the secret message (say, diagnosis details for telemedicine) in ASCII code $S_{Text_{ASCII}}$
Step-3 Scan cover image for each row
Step-4 Estimate the 2D wavelet coefficients for the first level using HAAR filter $(LL1), (HL1), (LH1)$, and $(HH1)$.
Step-5 Estimate the 2D wavelet coefficients for the second level using HAAR wavelet filter $(LL2), (HL2), (LH2)$, and $(HH2)$.
Step-6 Initiate a Loop
Hide $S_{Text_{ASCII}}$ using LSB embedding concept.
Initiate AGA-OPAP for adaptive pixel optimization and RS-Attack resilient LSB embedding.
EndLoop
Return Stego-Image
End
```

Algorithm 2 2D-DWT-2L Analysis and LSB Embedding

Unlike major conventional Hybrid Cryptography and Steganography models where authors have either focused on increasing embedding capacity or the basic histogram sensitive quality preserve, our proposed VIHCS model intends to retain maximum image data quality as well as security against recently acknowledged online attacks such as RS-Analysis or steganalysis. To achieve it, we have developed a novel and robust EC-assisted LSB embedding concept, where AGA intends to fit $S_{Text_{ASCII}}$ in such a manner that it doesn't introduce any significant entropy or visual trait signifying the presence of secret data.

5.2.2. AGA-OPAP Assisted LSB Embedding and Optimization

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

In this research, AGA has been applied to enhance image quality, embedding capacity as well as 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 to avoid those attacks which use either visual changes or statistical changes to detect hidden information or secret information within the cover image during transmission. Considering RS-Analysis, also called steganalysis attack condition which employs statistical features to detect the presence of hidden information in multimedia data under transmission; in our proposed VIHCS model we have considered RS parameters and PSNR sensitive LSB embedding to ensure optimal data security. The detailed discussion of the proposed embedding model is given as follows:

5.2.2.1. RS Analysis (Steganalysis)

In RS analysis or steganalysis approach, there are three distinct kinds of block flipping; Positive flipping (F_1), Negative flipping $(\mathrm{F}_{-1})$and Null flipping (F_0). Noticeably, F_1 signifies the transformation association in between the $2\mathrm{i}$ and $2\mathrm{i}+1$ pixels (say, 0-1, 2-3,…, 254-255), which is equivalent to the LSB coefficient. Similarly, the transformation association in between $2\mathrm{i}$ and $2\mathrm{i}-1$ pixels (say, -1, -1-0, 1-2,…255-256) signifies the negative flipping F_{-1}. Thus, the association between positive and negative flipping follows (4).

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

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

$$F_0(x) = x \quad (5)$$

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

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

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

The group G would remain consistent 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. In this process, at first, the input multimedia data (here, 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 certain random (say, Zigzag) manner. Here, the correlation amongst the pixel is obtained using a discrimination function, defined in (7).

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

In (7), the variable x states the value of the pixel, while the total number of pixels is given by n. Here, the resulting value of f signifies the spatial correlation between the neighboring pixels. Noticeably, 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., $M(1), M(2), \dots, M(n)$) either 0 or 1. On contrary, for non-positive flipping, we apply 0 or -1 for each block of the input image. Now, processing flipping over each block, we estimate $f\big(F(G)\big)$ 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}. Because in the natural images, the total number of above-stated blocks after performing flipping follow the following associations.

$$R_m \approx R_{-m}, S_m \approx S_{-m} \text{ and } R_m > S_m,\ R_{-m} > S_{-m} \qquad (8)$$

Typically, the difference between R_m and R_{-m} increases as per the size of the embedding message. Similarly, the difference values of S_m and S_{-m} too increase with an increase in embedding text. Such facts help attackers on a cloud platform or environment to detect the presence of hidden information that can result in a significant loss of data privacy. Considering it as motivation, in this research the focus is made on developing a robust 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 an attack-resilient secure cloud communication model. To achieve it, in this paper, an AGA algorithm has been developed that intends to adjust pixels optimally $R_m \approx S_m, R_{-m} \approx S_{-m}$. A detailed discussion of the proposed AGA-based OPAP is given in the subsequent section.

5.2.2.2. AGA based OPAP

As already stated in the above section, to avoid any stego-information retrieval or data attack, we focus 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 multimedia (here, image) data 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', $f_{-}(B_1') = 90$, only when F is non-positive flipping. Similarly, for B_2', $f_{-}(B_2') = 150$.

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

$$A_1 = \begin{bmatrix} 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 0 \\ 2 & 2 & 0 & 2 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 0 & 2 & 0 & 2 & 0 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad (10)$$

$$A_2 = \begin{bmatrix} 2 & 2 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 2 & 0 & 0 & 0 \\ 2 & 0 & 2 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 2 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 2 & 2 & 2 & 2 \\ 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 2 & 0 & 0 & 2 \end{bmatrix} \qquad (11)$$

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, the RS-Analysis attack of steganalysis attack can be avoided in a cloud environment. To achieve it, in this paper we have applied an Adaptive Genetic Algorithm (AGA) 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 a significantly high fitness value is considered for the next generation. Noticeably, the fitness value of a candidate solution signifies its maximum likelihood of becoming or getting selected for breeding in the next generation. To reduce computational overheads caused due to increase search space, a 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 our proposed LSB embedding method, at first, the stego-image is split into 8×8 blocks, where each block is categorized and labeled 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 $f(B'_{+})$, $f(B'_{-})$ and $f(B)$.

Step-4: Process steps 1, 2 and 3 iteratively for 1000 generations and defines four distinct variables to classify the blocks by comparing $f(B'_{+})$, $f(B'_{-})$ 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}, states the number of occurrences when the block remains regular under the non-positive flipping.

P_{-S}, 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 labeling of the image blocks as per 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 the above-stated types.

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

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

5.2.3. Population Initialization

From the initial pixel or the first pixel, chose 3 adjoining pixels in each image block as the initial chromosome (Figure 4).

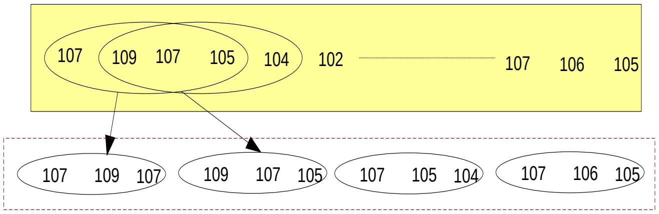


Figure 4 Selection of the Chromosomes

5.2.4. Reproduction and Mutation

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

5.2.5. Selection

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

$$Fitness = \alpha(e_1 + e_2) + PSNR \qquad (12)$$

In (12), the variable $\mathrm{e_1}$ states the likelihood of $\mathrm{f}(\mathrm{F_-}(\mathrm{C_i})) < f(\mathrm{C_i})$. Similarly, $\mathrm{e_2}$ signifies the likelihood of $\mathrm{f}(\mathrm{F_+}(\mathrm{C_i})) > f(\mathrm{C_i})$. The variable PSNR signifies the Peak Signal to Noise Ratio of the participating chromosome, while α presents a weight parameter that has been obtained empirically. Mathematically, PSNR has been obtained using (13).

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

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 that controls the visual quality of the input multimedia data and the secrecy of the secret text. For a specific value of α, higher the values of $e_1$and e_2, we hypothesize VIHCS 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 0.5.

5.2.6. Estimate

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

5.2.7. 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 that makes HCS more resilient to any attacks such as RS Analysis or steganalysis, which can achieve 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 VIHCS model, each block is labeled before initiating OPAP and thus, we reduce computational overheads significantly. Furthermore, the use of AGA reduces the exhaustive search operation and hence achieves computational-efficiency which makes it suitable for secure multimedia data transmission over cloud infrastructure.

5.3. 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 secret data as well as the original cover image by performing extraction using the 2D-DWT-2L method. In this method, at first Inverse DWT (IDWT) algorithm is applied over the received stego-image. An algorithmic-snippet of the extraction process is given Algorithm 3.

```
Input: Stego Image
Output: Secret message, Cover image.
Initiate the process
Step-1 Scan the stego image row-by-row
Step-2 Estimate the 2D wavelet coefficients for the 1-level of HAAR wavelet filter
Step-3 Estimate the 2D wavelet coefficients for the 2-level of HAAR wavelet filter
Step-4 Prepare message ""
Step-5 Initiate a loop
    Perform extraction of the text embedded in vertical coefficients and assign odd values =$LH2(x, y)$
    Perform extraction of the text embedded in horizontal coefficients and assign even values =$HH2(x, y)$
Step-6 End loop
Step-7 Reconstruct message $msg = append(odd, even)$
Step-8 Perform $IDWT$ for the constructed approximation which generates the original multimedia data or cover image
Step-9 Return text message as retrieved secret message and cover image.
End
```

Algorithm 3 Data Extraction

Once extracting the text data, we have synthesized the cover image from the reconstructed approximation by applying the IDWT technique for 2nd level followed by 1st level. Figure 5 elucidates the DWT synthesis process.

Now, considering the need to decrypt the secret text data from the cover image, similar to the encryption phase, Hybrid Cryptosystem applies AES and RSA algorithms to decrypt the secret data at the receiver. Receiving the stego image at the receiver unit, we decrypt the text using private key x to obtain the original secret message transmitted. The decryption algorithm used to retrieve the original secret data is given Algorithm 4.

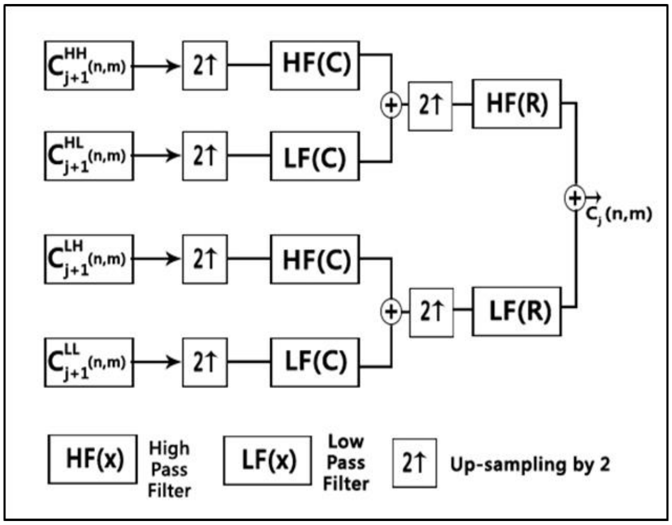


Figure 5 Extracting Encrypted Text from Images Showing the Procedure of Synthesis of DWT-2L

```
Input: Ciphertext received Cipher $_{Tx}$, key
Output: Secret message.
Initiate the process
Step-1 Split the received cipher text 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 plain text message
else
Insert even characters into even indices within plain text message.
End loop
Step-10 Retrieve original secret text and image transmitted.
End
```

Algorithm 4 Data Decryption

Thus, implementing the above-stated approach, we have obtained a computationally efficient VIHCS model which has been strengthened by employing cryptosystem enhancement as well as attack resilience (for example steganalysis or RS-Attack). The proposed system can be employed for secure data transmission over the cloud environment while ensuring optimal performance. A detailed discussion of the simulation results and their inferences is given in the subsequent section.

6. RESULTS AND DISCUSSIONS

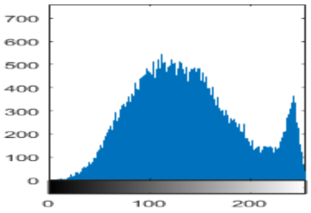
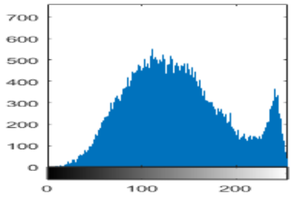
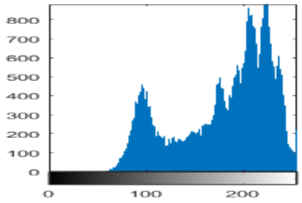
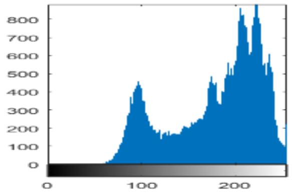
Considering the exponential rise in data communication in the cloud environment, this research focused on amalgamating strengths of the different security models such as cryptography and steganography, which is well known for multimedia data security. Realizing the communication demands and allied user interfaces, we modeled the overall system as transmitter and receiver, where the first (i.e., transmitter) intended to transmit the secret data embedded within the multimedia cover image. Noticeably, the transmitter terminal performs encryption, AGA-OPAP assisted LSB embedding, compression, and transmission. On contrary, the receiver performs extraction and decryption that eventually retrieves original secret data and cover image transmitted by the transmitter or user. 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 Windows-7 operating system. To assess the performance of the proposed VIHCS model, we used multiple images as the cover image and secret message of varied sizes.

The Hybrid Cryptography and Steganography (HCS) model can be effective or more efficient when it fulfills the following as shown in Table 1.

S.No.	Parameter	Definition
1.	PSNR	To preserve the quality of the multimedia data even after embedding secret text data, PSNR should be higher. The significant reduction in PSNR value can depict the presence of certain hidden information which can trigger attacker models to target and attack the data under the transmission.

2.	Entropy	It signifies the disturbance in the original image. To ensure minimum perceptibility, the HCS 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 the extent to which the secret text data can be embedded per unit of the cover image. An HCS 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 ($\boldsymbol{R_m - R_{-m}}$))	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 attackers 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 ($\boldsymbol{S_m - S_{-m}}$)	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 attackers or Steganalysis attacking modules to target data under the transmission. Lower the differences, higher the imperceptibility and resulting data security.
6.	Histogram Variations	It signifies the difference between the histogram patterns of the cover image as well as the stego image, before and after the embedding. Lower or negligible variations in the histogram graph show near-optimal embedding, which supports imperceptibility and hence attack resilience.

Table 1 Performance Criteria

S.No.	Dataset	Histogram of the cover image	
		Before	Post Embedding and OPAP
1. [44]			
2. [44]			

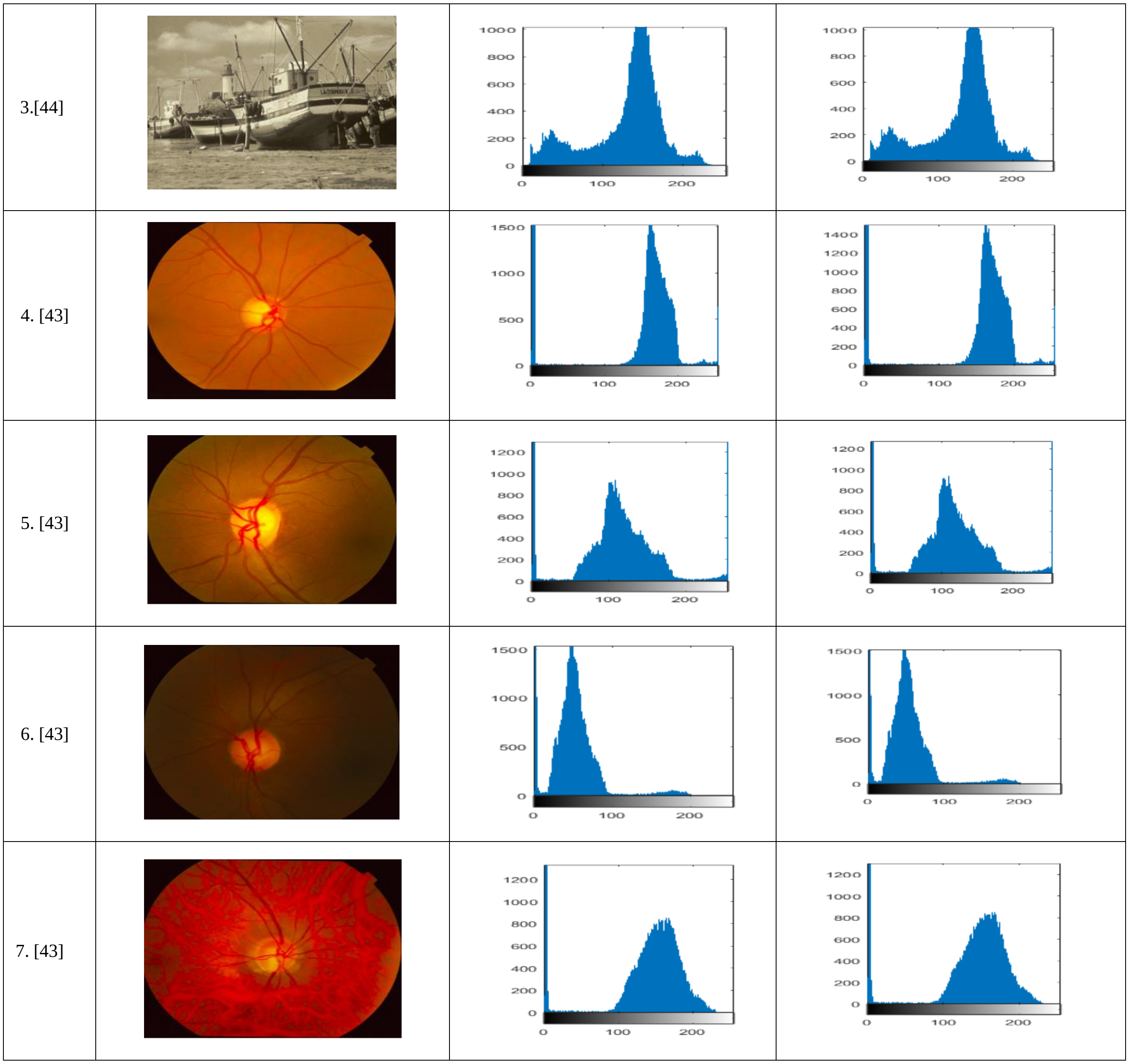


Figure 6 Histogram Pattern Analysis

Unlike major conventional researches, where authors have either focused on MSE, PSNR, or embedding capacity enhancement, in this research, we emphasize on accomplishing cumulative performance as mentioned in the above table. This as a result can accomplish optimal performance by the proposed VIHCS model to ensure an optimally secure communication environment for multimedia data over cloud platforms. As stated in Table 1, minimizing histogram pattern variations before and after message embedding in the cover image can help reducing visual perception or resulting tracking by attackers. Histogram variations take place 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, we introduced AGA-OPAP based LSB embedding that resulted in minimum histogram variations (Figure 6).

As depicted in Figure 6, our proposed VIHCS model exhibits negligible or near-zero variation in histogram after message embedding. Observing the results (Figure 6), it can be inferred that the proposed VIHCS model achieves optimal histogram pattern and retain its normalcy even after embedding, which supports the visual imperceptibility aspect for secure communication.

To assess the efficacy of the proposed VIHCS model, in this work we considered normal benchmark images such as Lena, Baboon, Boat [43] [44] as well as the medical images (DRISHTI-GS dataset). Here, the prime objective was to assess whether the proposed method can be effective 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 very critical healthcare data for "Diabetic Retinopathy", where even a single nerve can have significant information regarding the presence of diabetes.

Introduction of additional text (secret) data could cause entropy and hence quality degradation. However, VIHCS intended to optimize such entropy and ensure that stego-image (image after embedding) retains maximum possible image quality and originality. As depicted in Figure 6, image number 1, 2, and 3 are taken randomly from benchmark image dataset (Baboon, Lena and Boat dataset [44], respectively in *.jpg format), while images (4, 5, 6 and 7) are taken from DRISHTI-GS [43] dataset which is in *.png format. The second column presents the histogram pattern or the original image "before embedding", while the histogram pattern after OPAP assisted LSB embedding is given in the 3rd column. 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 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 (Fig. 6) are the cover images considered for the simulation and performance assessment.

In addition to the visual assessment through histogram analysis, we examined the performance in terms of the well-known statistical parameters such as PSNR (in dB) analysis, Regular and Singular coefficient variations in each block of the image due to LSB embedding, etc. Figure 7 presents the PSNR performance of the proposed VIHCS model for 250 bytes in the text (secret data) embedding. Observing the result in Figure 7, where the PSNR has been obtained for the text embedding size of 250 bytes, 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 it can be found that the proposed VIHCS 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 as given in (13) for the image processed after 2D-DWT-2L and post AGA-OPAP optimization.

The results obtained (Table 2) reveals that the proposed AGA-OPAP assisted LSB embedding method is of utmost significance towards retaining and optimizing image quality for quality-centric communication over a cloud environment.

As the image security process undergoes cipher generation which can significantly increase the disturbances across the image input. This, as a result, can cause an increase in image entropy which not only degrades (image) quality but also broadens the horizon for intruders to attack specific data. On the other hand, encryption imposes additional information to the multimedia data to make it complex for the intruder to distinguish the encrypted data and the original image information. In such cases, maintaining the optimal entropy with the data under transmission is a must. With this motive, in this paper, we estimated entropy for each encrypted data to retain quality-centric image security (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 signifies the intensity, and $P(I_i)$ signifies the probability of the intensity value I_i.

Analyzing the above results (Figure 8), it can be observed clearly that the spike in entropy is insignificant and thus keeps the image quality unchanged. It affirms the suitability of the encrypted images for critical applications such as healthcare (telemedicine) or critical data communication purposes. Similarly, we have examined the embedding capacity of the proposed model, which signifies the extent or the percentile to which a unit image can embed the text data (i.e., while ensuring no reduction in PSNR and correlation, and maintaining low entropy). Figure 9 presents the embedding capacity performance of the proposed model. Observing Figure 9, it can be easily found that the proposed method achieves a significantly large enhancement in the embedding capacity post-optimization. This can be because of the robustness of the proposed OPAP concept, which ensures optimal embedding while retaining entropy low and PSNR high, which are the key objectives of the employed AGA heuristic model. Thus, the results obtained signify the suitability of the proposed model for large-scale size encryption and secure communication purposes. This is the matter of fact that the addition or more secret information (text data) in the image might impose high entropy that eventually could lead to a reduction in image quality (i.e., PSNR).

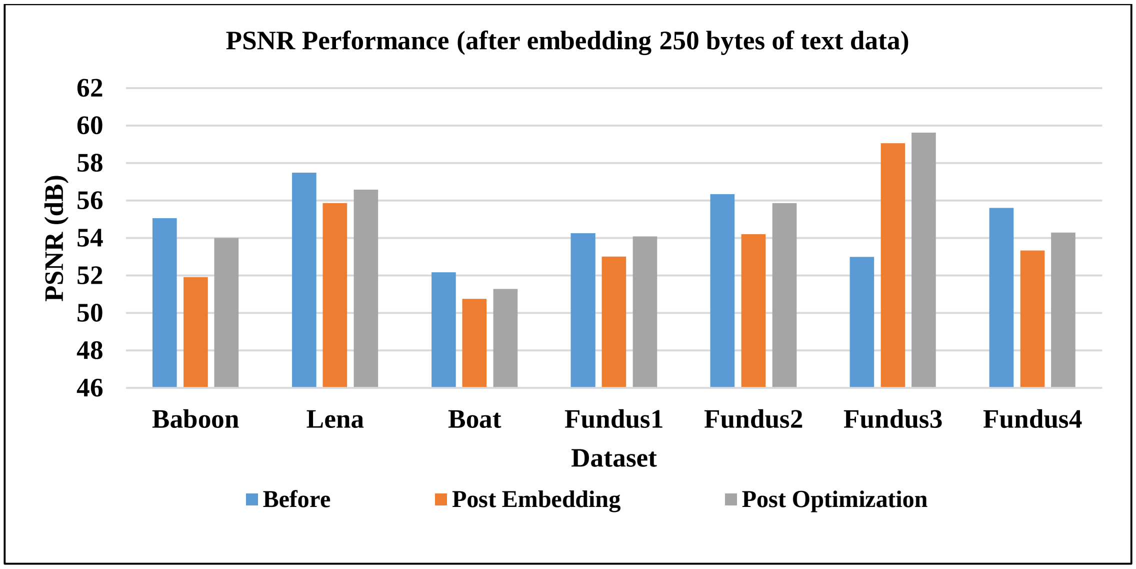


Figure 7 PSNR Performance (After Embedding 250 Bytes of Text Data)

Dataset	Data Size (bytes)	PSNR (dB)		
		Before	Post Embedding	Post Optimization
Baboon	250	55.0600	51.9200	54.0053
	500	58.8630	56.2003	57.8942
	1000	56.7491	55.8990	56.1804
Lena	250	57.4873	55.8762	56.5852
	500	53.1041	52.0072	52.9183
	1000	55.4901	54.0700	55.1003
Boat	250	52.1850	50.7611	51.2970
	500	56.8931	55.4180	55.9814
	1000	56.2443	55.0134	55.9993
Fundus1	250	54.2667	53.0110	54.1010
	500	52.2442	51.6320	52.1248
	1000	58.0012	57.4021	57.8732
Fundus2	250	56.3450	54.2101	55.8701
	500	59.1251	57.3427	58.6391
	1000	58.8422	56.1120	58.1297
Fundus3	250	53.0070	59.0629	59.6255
	500	56.0367	53.6730	54.9834
	1000	54.5259	52.1147	53.5895
Fundus4	250	55.6216	53.3414	54.3060
	500	58.8736	56.5290	57.9201
	1000	57.9910	56.3019	57.1003

Table 2 PSNR Performance over Different Sizes of the Secret Text Data

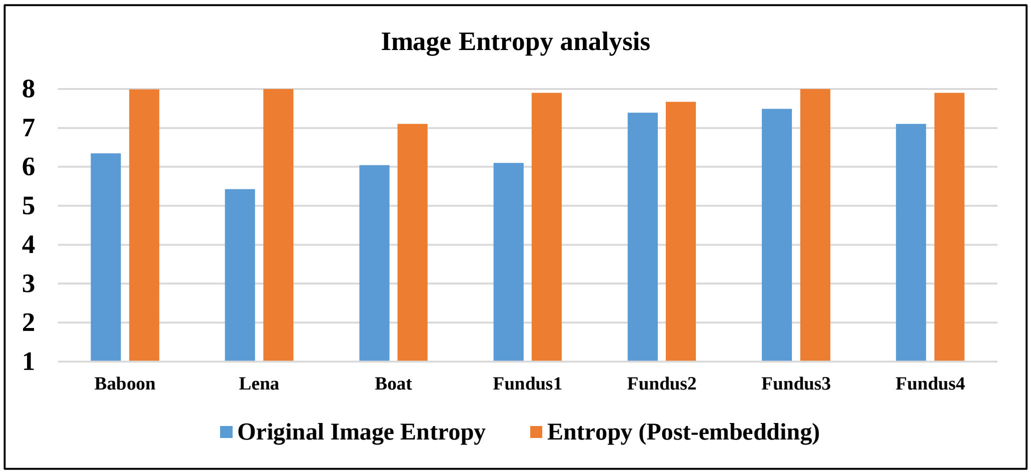


Figure 8 Image Entropy Analysis

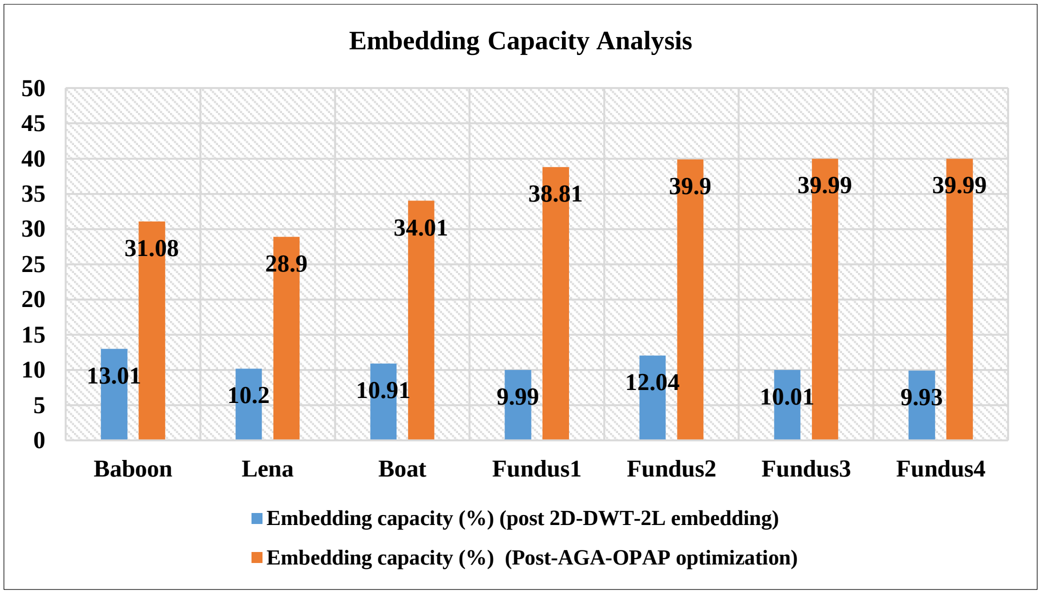


Figure 9 Embedding Capacity Analysis

In such a case, it is significant to assess whether the inclusion of the proposed AGA-OPAP assisted LSB embedding helps retaining maximum possible image quality even after large secret data embedding. With this motive, in this paper, we assessed the performance for the different sizes of the secret text data to be embedded in the cover image. Observing the results (Table 2) it can easily be found that though with an increase in secret data size (to be embedded into the cover image), the PSNR decreases; however the use of 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 can be vital to ensure higher data embedding inside the cover image without imposing any significant quality degradation or visual traits, which might invite intruders to attack over uncertain cloud communication channels or allied networks.

In addition to the PSNR assessment, in this research, we have considered the probability of statistical-assessment-based attack-proneness. In the majority of the existing HCS models, authors have either focused on enhancing embedding capacity or histogram pattern improvement. However, there are the attack models such as RS-Attack or Steganalysis attack which might explore into the multimedia data under the transmission to attack the specific data-carrying certain significant information or secret information. To alleviate such issues, we examined the variations in regular and singular coefficients per block of the image. As stated in Table 1, higher differences in the regular and singular coefficients can reveal the attackers about the presence of secret data within the multimedia data, and therefore maintaining lower differences can be advantageous.

Observing Table 3, it can be found that the proposed method achieves relatively lower differences in regular coefficient value $(R_m - R_{-m})$ and singular difference value$(S_m - S_{-m})$. It reveals that the proposed method can achieve a high level of visual imperceptibility that as a result can help to achieve secure data communication over a cloud channel. To assess the time efficiency of the proposed model for encryption, we applied MATLAB functions $*(tic - toc)$. We obtained overall execution time for the different datasets (Refer Table 2 for the different datasets and corresponding sequence). The execution time consumed over the different datasets is given in Table 4.

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	0.0064	0.0055	0.0058	0.0030	0.0016	0.0088
Lena	0.0036	0.0026	0.0033	0.0007	0.0113	0.0009
Boat	0.0040	0.0055	0.0066	0.0067	0.0016	0.0055
Fundus1	0.0092	0.0075	0.0077	0.0090	0.0077	0.0060
Fundus2	0.0030	0.0026	0.0035	0.0044	0.0113	0.0005
Fundus3	0.0040	0.0078	0.0020	0.0002	0.0074	0.0063
Fundus4	0.0084	0.0028	0.0062	0.0035	0.0113	0.0042

Table 3 RS Analysis (Secret Data Size 250 Bytes)

Dataset	Data Size (bytes)	Execution Time (ms)	
		Encryption	Decryption
Baboon	250	87.97	39.01
	500	72.60	33.01
	1000	70.63	32.97
Lena	250	89.45	41.00
	500	71.06	41.80
	1000	77.64	43.80
Boat	250	89.40	44.91
	500	88.48	43.31
	1000	82.26	43.73
Fundus1	250	71.31	39.92
	500	70.00	37.79
	1000	64.33	37.79
Fundus2	250	69.83	33.31
	500	69.91	33.67
	1000	69.91	33.55
Fundus3	250	71.01	38.89
	500	71.01	38.41
	1000	71.20	39.00
Fundus4	250	68.88	32.87
	500	71.60	39.18
	1000	76.00	41.47

Table 4 Execution Time over Different Sizes of the Secret Text Data

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. We evaluated the efficacy of the proposed model in terms of the number of pixel changes (NCPR) and the unified average channel intensity (UACI). The high value of NPCR and UACI typically means higher randomness and therefore high tolerance to any kind of differential attack [45].

Results of the randomness test with a higher NCPR value confirm the purpose of the proposed method's attack resistance. UACI also affirms our proposed data security model's good result. The above-mentioned reliability thus ensures the efficacy of the proposed security model for any data transmission in real-time, including the purposes of our intended cloud communication.

Dataset	NPCR (%)	UACI (%)
Baboon	99.60	25.77
Lena	99.83	28.32
Boat	99.83	23.81
Fundus1	99.59	36.61
Fundus2	99.43	28.60
Fundus3	99.63	41.06
Fundus4	99.52	14.87

Table 5 NPCR and UACI Randomness Test

Recalling the overall design where the key goal of employing hybrid cryptosystems 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 our proposed model avoids providing any scope of visual perceptibility and maintains low entropy, high PSNR, it would be able to resilient any attack conditions. Additionally, as the implementation of AGA-OPAP was done to avoid any statistical attack probability such as steganalysis or RS-attack approaches, it can withstand any attack condition to ensure secure communication. To assess the quality of the decrypted image at the receiver side, we obtained the mean absolute error (MAE) value using (15).

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

Where Y_i'refers the calculated output, while Y_i states for the expected value. The results obtained for sample inputs (with 250 bytes of text input) are given in Table 6. The results (Table 6) signifies the robustness in terms of a very negligible error profile, which undoubtedly affirms its superior image quality (post-decryption).

Dataset	MAE (%)
Baboon	0.1968
Lena	0.0996
Boat	0.3001
Fundus1	0.3109
Fundus2	0.4111
Fundus3	0.1557
Fundus4	0.1904

Table 6 MAE Performance with Different Input Samples (250 Bytes of the Text Secret Data)

The performance of the proposed model is assessed against state-of-the-art approaches where these algorithms have been developed to secure data in medical images. For comparison we have chosen Fundus image after embedding 250 bytes of secret text data. Comparative results are shown in Figure 10, which shows that the proposed algorithm clearly shows better results. The proposed VIHCS for data security showed better performance than the existing algorithms.

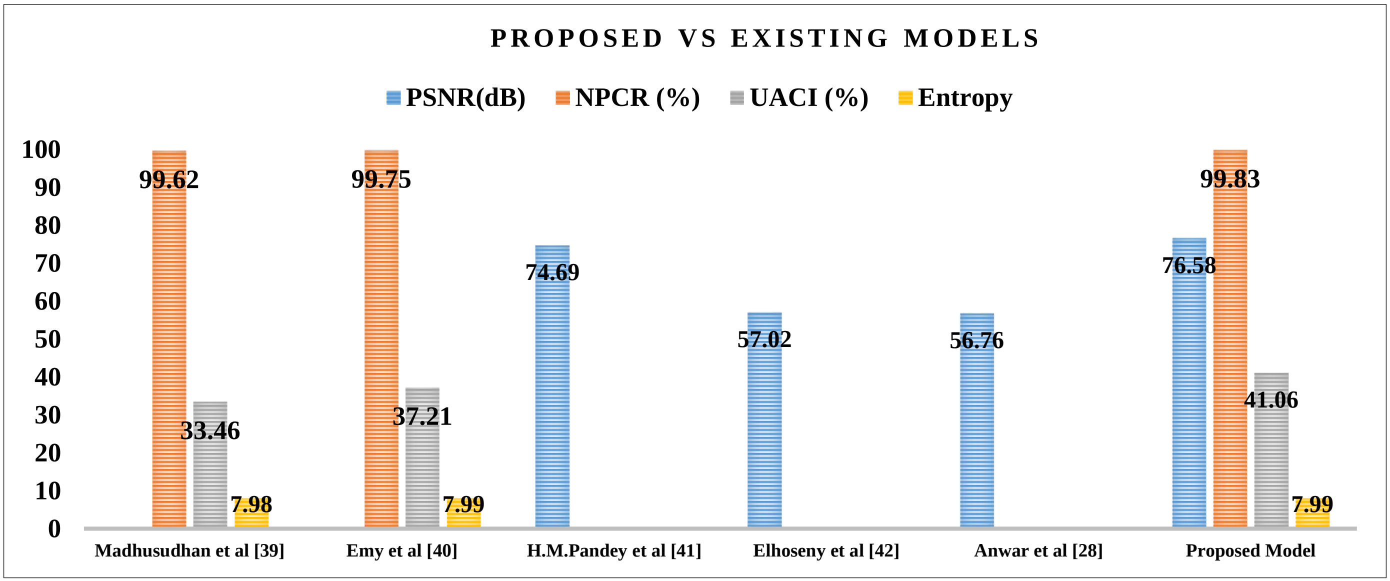


Figure 10 Comparison of Results

Thus, taking into consideration the proposed VIHCS model and its simulation-based performance, it can be inferred that the proposed system achieves optimal efficiency, which makes it suitable for secure data communication over the cloud environment. Observing the overall results, it can be found that the use of the HCS model with Hybrid Cryptosystems (AES and RSA together) and AGA-OPAP based embedding optimization can yield optimal VIHCS for secure multimedia communication over the cloud platform. Similarly, results indicate that the use of 64-RSA and 256-AES as strategically combined hybrid solution can be better towards VIHCS, though in this study we have not performed individual performance assessment for RSA and AES (distinctly).

Results obtained (Table 1 - Table 6) & (Figure 6 - 10) confirms that the use of AGA-OPAP has strengthened the VIHCS model to achieve optimal pixel adjustment which has eventually yielded PSNR enhancement, minimum histogram changes, or entropy. Besides, it has helped (due to PSNR and RS sensitive optimization) achieving optimal values for Regular and Singular coefficient values for each block. The simulation results reveal that the use of AGA-OPAP based LSB embedding has achieved maximum possible visual imperceptibility as well as data (image) quality which affirms the suitability of the proposed model for the cloud environment.

Considering overall structure, implementation mechanism and key goals, where the prime focus was made on achieving:

1. High PSNR and Low entropy (to preserve quality, see Figure 6, Table 2 and Figure 8)
2. Low-delay (to support time-efficient communication, see Table 4)
3. High embedding capacity (to enable resource-efficient secure communication, see Figure 9)
4. High visual quality and imperceptibility (to confuse or avoid any MITM attacks based on image quality and certain statistical calculations such as steganalysis, RS-attack, correlation information, etc for better attack-resiliency, see Figure 6).
5. High image quality (higher NCPR and UACI, see Table 5) and low MAE (see, Table 6).
6. The efficiency of the proposed model is examined alongside the existing algorithm where the results have been stated in Figure 10. The result reveals that the proposed algorithm achieved improved results related to the existing algorithms.

Observing the overall results and corresponding inferences, it can be inferred that a better or suitable programming paradigm for our proposed VIHCS 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 VIHCS 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.

7. CONCLUSION

Considering the exponential rise of data communication over the cloud environment, which is often considered as uncertain in this research the emphasis was made on developing a robust and efficient secure data transmission model. Unlike conventional approaches such as cryptosystems, this research intended to exploit the efficacy of both cryptosystems as well as steganography. However, realizing the fact that the majority of the classical approaches are prone to get attacked if used in conventional form, a hybrid cryptosystem was developed using RSA and AES cryptography algorithms. The use of these two algorithms and their strategic implementation towards secret data encryption and decryption strengthened the overall level of security and ensured that the secret information can't be retrieved easily. On the other hand, realizing the quality preserve aspect of steganography which is often used in image data security, an Adaptive Genetic Algorithm assisted OPAP was developed that optimized the least significant bit embedding over image-blocks. The AGA-OPAP model considered PSNR as well as Regular and Singular Coefficient values per block of the image as objective functions to perform secret message embedding and allied pixel adjustment (optimization). It affirms proposed AGA-OPAP model itself is a novel and robust approach to achieve better image quality, visual imperceptibility, and higher embedding capacity even without losing original quality. These all features make the proposed system suitable for numerous data communication purposes including cloud communication, healthcare data communication, IoT communication purposes, etc. MATLAB based model development and its simulation with different image datasets as well as secret text of varied sizes revealed that the proposed VIHCS model can be attack resilient (statistical assessment based attack models) and quality-centric (high PSNR) which make it suitable for secure communication over cloud platforms. The proposed VIHCS model can be resilient to the state-of-art attacking models such as RS-Attack, Steganalysis, etc. Summarily, the proposed VIHCS model is suitable for secure data transmission over a cloud platform. Though, the use of HCS is a novel concept, in the future focus can be made on designing a single lightweight cryptosystem with equivalent or better security provision for multimedia data.

REFERENCES

[1] R. K. Gupta and P. Singh, “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., vol. 3, no. 8, pp. 108-115, 2013.

[2] Anupam Kumar Bairagi, Rahamatullah Khondoker & Rafiqul Islam (2016) An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures, Information Security Journal: A Global Perspective, 25:4-6, 197-212, DOI: 10.1080/19393555.2016.1206640.

[3] Sajjad, M., Muhammad, K., Baik, S.W. et al. Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimed Tools Appl 76, 3519–3536 (2017). https://doi.org/10.1007/s11042-016-3811-6

[4] Darwish, A., Hassanien, A.E., Elhoseny, M. et al. The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. J Ambient Intell Human Comput 10, 4151–4166 (2019). https://doi.org/10.1007/s12652-017-0659-1

[5] Y. Xu, X. Zhao and J. Gong, "A Large-Scale Secure Image Retrieval Method in Cloud Environment," in IEEE Access, vol. 7, pp. 160082-160090, 2019, doi: 10.1109/ACCESS.2019.2951175

[6] Mersini Paschou, Evangelos Sakkopoulos, Efrosini Sourla, Athanasios Tsakalidis, Health Internet of Things: Metrics and methods for efficient data transfer, Simulation Modelling Practice and Theory, Volume 34, 2013, Pages 186-199, https://doi.org/10.1016/j.simpat.2012.08.002

[7] Muhammad Sajjad, Mansoor Nasir, Khan Muhammad, Siraj Khan, Zahoor Jan, Arun Kumar Sangaiah, Mohamed Elhoseny, Sung Wook Baik, Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities, Future Generation Computer Systems, Volume 108, 2020, Pages 995-1007, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.11.013.

[8] Laskar, Shamim. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems. 4. 57-68. 10.5121/ijdms.2012.4605.

[9] May Zaw, Z., & Phyo, S. W. (2015). Security Enhancement System Based on the Integration of Cryptography and Steganography. International Journal of Computer (IJC), 19(1), 26-39

[10] L. Yu, Z. Wang and W. Wang, "The Application of Hybrid Encryption Algorithm in Software Security," 2012 Fourth International Conference on Computational Intelligence and Communication Networks, Mathura, 2012, pp. 762-765, doi: 10.1109/CICN.2012.195.

[11] Parah S.A., Sheikh J.A., Ahad F., Bhat G.M. (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

[12] Li, L., Hossain, M.S., El-Latif, A.A.A. et al. Distortion less secret image sharing scheme for Internet of Things system. Cluster Comput 22, 2293–2307 (2019). https://doi.org/10.1007/s10586-017-1345-y

[13] B. Xue, X. Li and Z. Guo, "A New SDCS-based Content-adaptive Steganography Using Iterative Noise-Level Estimation," 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Adelaide, SA, 2015, pp. 68-71, doi: 10.1109/IIH-MSP.2015.80.

[14] Vipula Madhukar Wajgade, "Enhancing Data Security Using Video Steganography," International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.

[15] Marwa E. Saleh, Abdelmgeid A. Aly and Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques" International Journal of Advanced Computer Science and Applications (IJACSA), 7(6), 2016. http://dx.doi.org/10.14569/IJACSA.2016.070651

[16] M. E. Saleh, A. A. Aly, and F. A. Omara, "Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding," International Journal of Computer Science and Security (IJCSS), Volume (9), Issue (2), pp. 397 - 397, 2015

[17] A. Duluta, S. Mocanu, R. Pietraru, D. Merezeanu and D. Saru, "Secure Communication Method Based on Encryption and Steganography," 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, 2017, pp. 453-458, doi: 10.1109/CSCS.2017.70.

[18] Dhvani Panchal, "An Approach Providing Two Phase Security of Images Using Encryption and Steganography in Image Processing", 2015 IJEDR, Volume 3, Issue 4, ISSN: 2321-9939.

[19] Y. Leung and R. Y. Hou, "Unequal security protection for secure multimedia communication," 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), Osaka, 2015, pp. 570-571, doi: 10.1109/GCCE.2015.7398667.

[20] J. Li, X. Guo, Y. Yu, Q. Tu and A. Men, "A robust and low-complexity video fingerprint for multimedia security," 2014 International Symposium on Wireless Personal Multimedia Communications (WPMC), Sydney, NSW, 2014, pp. 97-102, doi: 10.1109/WPMC.2014.7014798.

[21] D. E. M. Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography," 2014 International Conference on Computer and Communication Engineering, Kuala Lumpur, 2014, pp. 288-291, doi: 10.1109/ICCCE.2014.88.

[22] V. Hajduk, M. Broda, O. Kovac and D. Levicky, "Image steganography with using QR code and cryptography," 2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA), Kosice, 2016, pp. 350-353, doi: 10.1109/RADIOELEK.2016.7477370.

[23] M. Mukhedkar, P. Powar and P. Gaikwad, "Secure non real time image encryption algorithm development using cryptography & steganography," 2015 Annual IEEE India Conference (INDICON), New Delhi, 2015, pp. 1-6, doi: 10.1109/INDICON.2015.7443808.

[24] M. S. Alam, "Secure M-commerce data using post quantum cryptography," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 649-654, doi: 10.1109/ICPCSI.2017.8391793.

[25] N. Kumar and S. Agrawal, "An efficient and effective lossless symmetric key cryptography algorithm for an image," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, 2014, pp. 1-5, doi: 10.1109/ICAETR.2014.7012788.

[26] S. F. Mare, M. Vladutiu and L. Prodan, "Secret data communication system using steganography, AES and RSA," 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), Timisoara, 2011, pp. 339-344, doi: 10.1109/SIITME.2011.6102748.

[27] P.V.Nithyabharathi, T.Kowsalya, V.Baskar, "To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES", IJSETR, Volume 3, Issue 2, February 2014.

[28] Anwar, Asmaa & A.Ghany, Kareem & Elmahdy, Hesham. (2015). Improving the security of images transmission. International Journal of Bio-Medical Informatics and e-Health. 3. 7-13.

[29] Xin Liao, Jiaojiao Yin, Sujing Guo, Xiong Li, Arun Kumar Sangaiah, Medical JPEG image steganography based on preserving inter-block dependencies, Computers & Electrical Engineering, Volume 67, 2018, Pages 320-329, ISSN 0045-7906. https://doi.org/10.1016/j.compeleceng.2017.08.020.

[30] Balakrishnan Ramalingam , Amirtharajan Rengarajan , John Bosco Balaguru Rayappan , Hybrid Image Crypto System for Secure Image Communication- A VLSI Approach, *Microprocessors and Microsystems* (2017), doi:10.1016/j.micpro.2017.02.003

[31] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan and R. Amirtharajan, "DNA Chaos Blend to Secure Medical Privacy," in IEEE Transactions on NanoBioscience, vol. 16, no. 8, pp. 850-858, Dec. 2017, doi: 10.1109/TNB.2017.2780881.

[32] Mansour, R.F., Abdelrahim, E.M. An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. *Multidim Syst Sign Process* **30,** 791–814 (2019). https://doi.org/10.1007/s11045-018-0575-3

[33] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319263.

[34] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim and S. Islam, "Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography," 2019 7th International Conference on Mechatronics Engineering (ICOM), Putrajaya, Malaysia, 2019, pp. 1-6, doi: 10.1109/ICOM47790.2019.8952061.

[35] Chidambaram, N., Raj, P., Thenmozhi, K. *et al.* A cloud compatible DNA coded security solution for multimedia file sharing & storage. *Multimed Tools Appl* **78,** 33837–33863 (2019). https://doi.org/10.1007/s11042-019-08166-z

[36] Shilpi Harnal, R.K. Chauhan, "Hybrid Cryptography based E2EE for Integrity &Confidentiality in Multimedia Cloud Computing", IJITEE, Volume 10, Issue 8, August 2019.

[37] Stoyanov B, Stoyanov B. BOOST: Medical Image Steganography Using Nuclear Spin Generator. *Entropy*. 2020; 22(5):501.

[38] Abd-El-Atty B, Iliyasu AM, Alaskar H, Abd El-Latif AA. A Robust Quasi-Quantum Walks-based Steganography Protocol for Secure Transmission of Images on Cloud-based E-healthcare Platforms. *Sensors*. 2020; 20(11):3108

[39] Madhusudhan, K.N., Sakthivel, P. A secure medical image transmission algorithm based on binary bits and Arnold map. *J Ambient Intell Human Comput* (2020). (online first) https://doi.org/10.1007/s12652-020-02028-5

[40] Emy Setyaningsih, Retantyo Wardoyo, Anny Kartika Sari, Securing color image transmission using compression-encryption model with dynamic key generator and efficient symmetric key distribution, Digital Communications and Networks, 2020, (online first) ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2020.02.001.

[41] Hari Mohan Pandey, Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography, Future Generation Computer Systems, Volume 111, 2020, Pages 213-225, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.04.034.

[42] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in *IEEE Access*, vol. 6, pp. 20596-20608, 2018.

[43] A Comprehensive Retinal Image Dataset for the Assessment of Glaucoma from the Optic Nerve Head Analysis. Sivaswamy J, S. R. Krishnadas, Arunava Chakravarty, Gopal Dutt Joshi, Ujjwal and Tabish Abbas Syed , JSM Biomedical Imaging Data Papers, 2(1):1004, 2015.

[44] Input images available URL, "htttps://homepages.cae.wisc.edu/~ece533/images/".

[45] Y. Wu, J. P. Noonan, S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011, pp.31-38, 2011.

[46] Rayappan, D., Pandiyan, M. Lightweight Feistel structure based hybrid-crypto model for multimedia data security over uncertain cloud environment. Wireless Netw (2020). https://doi.org/10.1007/s11276-020-02486-x.

Authors

Denis R has obtained a Bachelor of Science (B.Sc.) from Loyola College (Autonomous), Madras University, Chennai, TN, India, and Master of Computer Applications (MCA) from Sacred Heart College (Autonomous), Tirupattur in the year 2006 and 2009 respectively. Presently, he is pursuing a Ph.D. in Computer Science at Periyar University, Salem, TN, India. He has published research papers in peer-reviewed journals and conferences, one Indian Patent, and authored two books (Java Programming – for Core and Advanced Users, ISBN: 9789386235329 | Year: 2018 & Constructive Java Programming ISBN: 9789389211771 | Year: 2020-2021) by Universities Press (India) Pvt. Ltd, Hyderabad. His research interests include Data Security and Privacy, Cryptography Algorithms, Big Data Analytics, Data Mining, and Bio-inspired algorithms.

Madhubala P obtained a Ph.D. in Computer Science from Mother Teresa Women's University, Kodaikanal, TN, India in the year 2017. She is currently a Assistant Professor at the Research Department of Computer Science, Don Bosco College of Arts and Science, Dharmapuri, TN, India since 2007. Also, she is the University nominee for the Board of Studies of the BCA department at Sacred Heart College (Autonomous), Thiruvalluvar University, Tirupattur, TN, India. She has published more than 13 research papers in peer-reviewed international journals and conferences. Her research interests include Cloud Computing, Wireless Sensor Networking, Data security, advanced data mining, and Artificial Intelligence. She has 19 years of teaching experience and 8 years of Research Experience. Currently, she is guiding four Ph.D. students.