ANALYTICAL AND INTEGRATED FRAMEWORK FOR PRIVACY PRESRVATION OF IMAGES IN CLOUD ECOSYSTEM

Chhaya S Dule

Research Scholar, Department of Computer Science and Engineering,
GSSS Institute of Engineering and Technology for Women, Mysore,
Visvesvaraya Technological University, Belgaum, Karnataka, India
Assistant Professor, Department of Computer Science and Engineering,
Dayananda Sagar University, Bangalore ,India
chhaya.s-cse@dsu.edu.in

Dr. Roopashree H R

Research Supervisor and Associate Professor, Department of Computer Science and Engineering,
GSSS Institute of Engineering and Technology for Women, Mysore
Visvesvaraya Technological University, Belgaum, Karnataka, India
roopashreehr@gsss.edu.in

Abstract

Privacy preservation is always a potential concern while storing or transmitting images with sensitive information within them. A review of existing privacy preservation techniques shows the potential usage of deep learning, adoption of highly sophisticated encryption, lack of packetization scheme, and focus on a singular attack. Therefore, the proposed study presents a novel analytical framework for the privacy preservation of image data in the cloud environment. A novel and simplified mathematical model with layer-based operation is constructed, which facilitates appending image chunks with digital security code and encryption token using a hash to generate a hash vector of an image with a higher degree of secrecy. An extensive analysis is carried out over different datasets of images to find that the proposed scheme offers consistency in its performance and a significant balance between security and computational performance in contrast to frequently exercised privacy preservation schemes. The study outcome exhibited 59% overhead reduction, 25% enhanced signal quality, 65% better resolution, and 40% faster execution time in contrast to the existing scheme.

***Keywords*: Cloud Environment; Image Privacy Preservation; Mathematical Model ; Secrecy.**

1. Introduction

Information is critical in every application sphere, irrespective of its deployment scenario. This information is required to be protected with suitable security techniques. Various approaches can safeguard personal information in text form [Debnath *et al.*, 2020; Kamal *et al.*, 2021]. However, with the advancement of technologies and communication, image plays a prime role in carrying important information. Such images consist of sensitive private details that are quite vulnerable to intrusive or malicious activity [Jiao *et al.*, 2019]. Hence, privacy preservation techniques have evolved to safeguard this personal and private information whose accessibility is restricted to the only legitimate user [Chai *et al.*, 2022]. Conventional privacy preservation techniques consist of masking the part of sensitive information as well as other frequently adopted techniques are blurring and pixelating the private information [Zhang *et al.*, 2021]. While protecting private information within an image, encryption is the widely adopted technique that cipher the image so that its private information is quite hard to disclose even to service providers [Guo et *al.*, 2020]. However, adopting encryption techniques comes at the cost of a computational burden. Currently, various study approaches are being implemented to ensure privacy protection for the images [Boulemtafes *et al.*, 2020; Cunha *et al.*, 2021; Liu *et al.*, 2020; P. Yang *et al.*, 2020]. However, existing approaches are characterized by various shortcomings, forcing the research community to keep exploring more robust solutions. Some of the challenges of existing approaches are: i) unable to differentiate the important and non-important content to be distorted for securing private details, ii) highly challenging towards retrieving the original information, iii) adoption of encryption techniques is found with significant clarity towards the protected contents

and hence violates the imperceptibility of private details, iv) adoption of region-of-interest based approaches are highly dependent on the scalable performance of encryption image, and it is quite limited to usage over the similar form of an image [Alkhelaiwi *et al.*, 2021; Chen *et al.*, 2020; Deng *et al.*, 2021; Raynal *et al.*, 2020; M. Zheng *et al.*, 2019].

Moreover, the problem of privacy vulnerability is highly vulnerable when exposed to various threats in a wireless environment or large-scale distributed environment, e.g., the cloud (Li *et al.*, 2020). The recent work, e.g. (Cai *et al.*, 2022; Kiya *et al.*, 2022; Zhou *et al.*, 2022) offers some potential guidelines for developing a framework for the privacy preservation of any form of data. According to such guidelines, an alternative solution to conventional encryption techniques is needed. This could balance the computational overhead as well as security performance. Further, the modeling must be carried out in such a way that it offers higher resiliency toward any form of attack. Therefore, the proposed study introduces a novel computational framework that can facilitate the effective privacy preservation of any form of an image.

The contributions of the proposed scheme are as follows:

- The proposed scheme introduces a lightweight encryption scheme unlike any conventional techniques
- The scheme uses hashing technique to append the hash with the image and digital security token over multiple layers of image data
- Mathematical modelling is presented which facilitates an effective resource allocation to support the encryption and forwarding of data,
- Deployed on wireless nodes operation on the cloud environment, the scheme offers security with optimal performance.

The organization of the study is as follows: Section 2 discusses existing privacy preservation approaches, followed by highlights of problems in Section 3. Section 4 briefs the adopted research methodology, while Section 5 discusses system design concerning mathematical models and algorithms. Section 6 discusses an accomplished outcome, while Section 7 briefs the study's conclusion.

2. Literature Review

Image being frequently utilized in various application; it is highly prone to be subjected to intrusive activities. From the context of privacy preservation of images, there are various studies that has addressed this problem. The recent work carried out by [Lida and Kiya, 2020] have used encryption-based methodology toward preserving privacy factors of an image during retrieval process. The presented scheme has deployed image descriptors in order to facilitate retrieval process. Study towards privacy preservation is carried out by [Janani and Brindha, 2022] where a cloud database with encryption has been formulated as a solution. The scheme also carries out similarity matching in secured form in order to deploy efficient secrecy. Adoption of deep learning is reported in work of [Huang *et al.,* 2022] where an encryption algorithm is formulated for securing image. The uniqueness of this study is towards developing a learnable encryption algorithm where the focus is towards maintaining privacy towards training images. The work carried out by [Bi *et al.* 2022] have developed a scheme where privacy of image is emphasized along with computation and storage of a color image. The contribution of this study is towards offering a secured extraction of feature using orthogonal moments. Adoption of blockchain is another frequently adopted technique towards ensuring image privacy. The work carried out by [Zerka *et al.*, 2020] have developed an integrated scheme of blockchain and machine learning of distributed chain form in order to develop a secure centralized scheme. This study model is meant for allowing the training operation to be carried out dynamically with respect to learning models.

The work carried out by [Yang *et al.*, 2020] has also used homomorphic encryption towards safeguarding images. The technique has also used extraction of feature vector using histogram-based approach while the encryption is carried out in order to generate encrypted kernels. Further, support vector machine has been implemented for training these kernels. A unique study model has been presented by [Sun *et al.* 2022] where compressed sensing technique has been used for privacy preservation of medication images. Assessed over selected plaintext attack, the proposed scheme performs realization of the privacy preservation over vulnerable cloud server. The presented study also includes integrated usage of an arbitrary padding, permutation, linear transformation in order to offer better security efficiency. The work of [Zheng *et al.*, 2021] have presented a technique that uses deep learning as well as denoising technique in order to offer better privacy over cloud environment. The study of [Ma *et al.*, 2021] have also used deep learning approach over cloud for ensuring better privacy preservation. According to this model, deep learning is applied over encrypted data considering numerous secret keys while stochastic gradient descent is used for performing training process. The authors in [Hassanpour *et al.*, 2022] have used continual learning approach in order to bridge the tradeoff between utility and privacy. The idea of this work is towards resisting any possibilities of catastrophic forgetting while performing learning operation. The work carried out by [Yang *et al.,* 2020] has implemented a plaintext encryption scheme for facilitating a unique reversible data hiding scheme. The study has considered medical image for analysis for minimizing attention of an attacker. The study presented by [Zhou *et al.,* 2020] have used region-of-interest based scheme in order to perform encryption. The study has also implemented neural network with chaos theory in order

to diffuse the region of interest. Adoption of Hahn moment is carried out by [Yang *et al.*, 2018] where an encryption is carried out over the extracted features of an image. The study has used homomorphic encryption using mathematical modelling. Adoption of deep neural network was witnessed in work of [Sirichotedumrong *et al.*, 2019] where an encrypted images were used for training the deep neural network model in order to assists the classification process of an image. The work by [Puteaux and Peuch 2021] have developed an encryption scheme where the noisy image is subjected to correction. Using Advanced Encryption Standard, the ciphering of the noisy block of an image is carried out. The study of [Cheng *et al.*, 2022] have used watermarking scheme for ensuring privacy preservation of an image evaluated over the edge network. The model has used homomorphic encryption as well as discrete wavelet transform where a singular value decomposition has been carried out over the edge server. In the work of [Hasan *et al.*, 2021] implemented an encryption technique considering the user case of securing medical images. A permutation scheme has been implemented towards securing the image data.

The work by [Nakamura *et al.*, 2019] presented a framework towards recognition of images without using any form of encryption towards privacy protection. According to this scheme, the visual features of an image is extracted and subjected to the transformation which render server not being able to identify them. The work discussed by [Zhang *et al.*, 2017] have constructed a framework that can offer privacy while performing image service over cloud environment. The work carried out by [Ko *et al.*, 2020] have used deep learning scheme towards perform de-identification of a structural image. The idea of this work is to prove the accuracy for classification process is like that of deep learning performance without using encrypted image. In the study of [Sheidani *et al.*, 2021] have used reversible data hiding scheme along with using elliptical curve encryption towards resisting chosen plaintext attack. Adoption of deep learning is also reported in work of [Yi *et al.*, 2021] where encoding and deep learning scheme has been implemented in order to facilitate image classification. The model discussed by [Jiang *et al.,* 2021] have used encrypted domain over image feature in order to secure the privacy information within the image. Study towards encrypted domain was also carried out by [Mohanty *et al.*, 2020] where the privacy details of camera fingerprint is protected using Boneh-Goh-Nissim Scheme. The study also claimed of mitigating the privacy leakage. The work by [Ito *et al.*, 2021] have used deep neural network along with a transformation network for securing the visual attributes of an image. The summary of the existing approaches is given in Table 1.

Approaches	**Contributors**	**Advantage**	**Limitation**
Encryption	[Iida and Kiya 2020]; [Janani and Brindha 2022]; [Yang *et al.*, 2020]; [Puteaux and Puech 2021]; [Hasan *et al.,* 2021]; [Sheidani *et al.,* 2021]; [Jiang *et al.,* 2020]; [Mohanty *et al.,* 2021]	Simplified approach	Sophisticated ciphering
homomorphic encryption	[Bi *et al.,* 2022]; [Yang *et al.*, 2020]; [Cheng *et al.*, 2022]	Secured feature extraction, Robust security against privacy attacks	Computationally extensive process
Encryption with deep learning	[Huang *et al.*, 2022]; [Ma *et al.,* 2021]; [Sirichotedumrong *et al.*, 2019]; [Zhou *et al.*, 2020]; [Yi *et al.*, 2021]; Zerka *et al.*, [2020]; Zheng *et al.*, [2021]	Offers privacy for trained image, Effective security towards target ROI	Dependent on the trained dataset, Inaccuracies still exist for varied images
Transformation of extracted feature	Nakamura *et al.*, 2019]	Non-encryption based	Couldn't protect against lethal attacks
Deep learning	[Ko *et al.*, 2020]; [Ito *et al.*, 2021]	Higher accuracy in attack detection	Specific to one form of attack

Table 1 Summary of Existing Approaches

After reviewing the existing approaches in the prior section, conclusive remarks are drawn regarding identifying significant research problems.

- **Potential Usage of Deep Learning:** Existing deep learning scheme over the encryption domain (Alkhelaiwi *et al.*, 2021], Huang *et al.*, 2022] is noted with highly iterative, demand training data and learning operations, and does not offer scalable performance for various ranges of an image.
- **Adoption of highly sophisticated encryption:** Adoption of various key-based encryption [Jiang *et al.*, 2020], [Ma *et al.*, 2021], homomorphic encryption [Bi *et al.*, 2022], Yang *et al.*, 2020], [Cheng *et al.*, 2022], elliptical curve encryption [Sheidani *et al.* 2021] offers security at the cost of the computational burden. Hence, a lightweight encryption algorithm is needed to facilitate its execution over resource constraint devices.
- **Lack of packetization scheme**: Most of the existing privacy preservation approaches have been carried out/assessed using one type of image with a similar configuration. There is no evidence of any scheme to support multiple types of images for privacy protection. Hence, until and unless the image is split into smaller

packets or without developing any distributed encoding scheme, the encrypted image will be challenging to store and transmission.

- **Focus on a singular attack:** Most existing studies encounter incompatibility issues when exposed to the variable deployment environment. For example, when a wireless node is exposed to the internet or cloud, they are vulnerable to known and unknown attacks. There is no report of any studies that support resisting multiple forms of attacks.

Therefore, all the above-stated research problems are addressed in the proposed study. The next section discusses the problem solution to mitigate the above-reported problem.

3. Methodology

The prime ideology of the proposed scheme is to develop an integrated analytical framework that can offer effective privacy preservation of the images in the cloud environment. To develop this objective, the proposed scheme introduces a novel integrated model which can evaluate the performance of different kinds of images containing privacy constructs. The architecture of the proposed scheme is exhibited in Fig.1

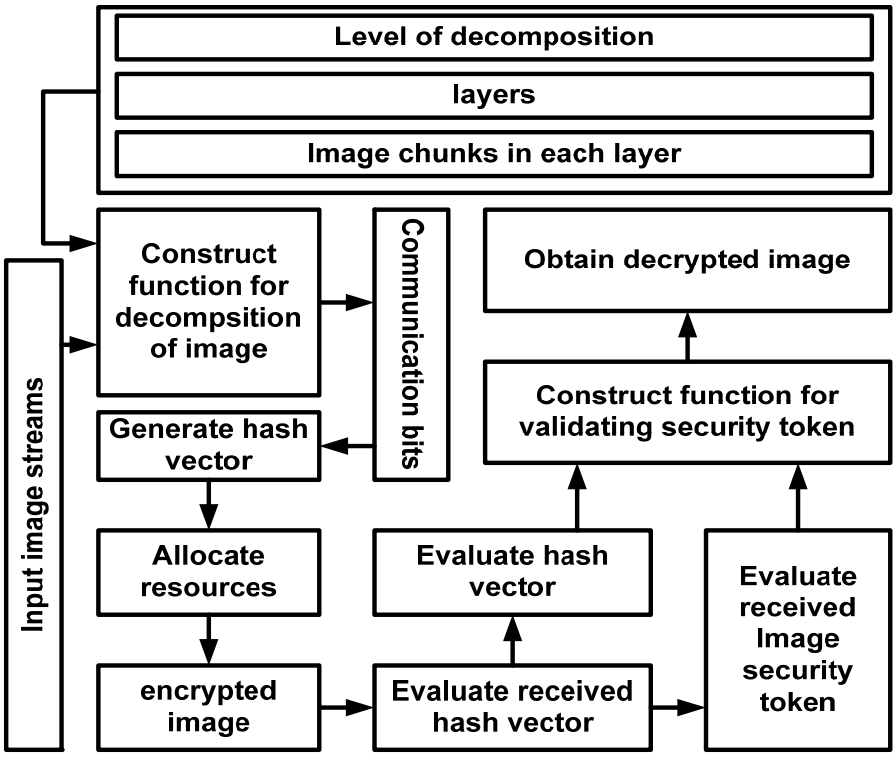


Fig. 1. Architecture of Proposed Privacy Preservation of Image

According to Fig.1 the proposed scheme uses mathematical modeling and considers the stream of input image subjected to a novel decomposition operation without losing an image's essential pixel characteristic. A novel function is constructed that generates a communication bit further transformed into hash vectors. The study model also contributes towards allocating computed resources for facilitating a wireless node under a cloud environment to transmit the image. The acquired encrypted image is evaluated for its hash vector, followed by the evaluation of the image security token. A discrete function validates the acquired security token, resulting in the decrypted image. A closer look into this architecture will show that the proposed system is designed with progressive operation without including iterative and complex mathematical schemes, as noted in existing schemes. The proposed study model is to develop a lightweight encryption algorithm that can be executed on any wireless device with restricted resource availability operating over distributed cloud environment. The next section further elaborates on this architecture concerning mathematical model and algorithm to highlight the effectiveness of the proposed privacy preservation scheme. The proposed system emphasizes designing a secure cloud environment to perform the security management of various ranges of image-based data. It should be noted that the proposed system caters to dual security demands, i.e., securing the storage units where the image is reposited and constructing a secure communication channel for the propagation of images. This section elaborates on the system design concerning mathematical modeling and algorithm discussion to illustrate the operational planning of implementing the proposed scheme.

4. System Design

The prime component of the model is a digital security code, image data, and encryption security token. The proposed methodology also contributes towards mathematical modeling, which appends image data with digital security code and encryption token, unlike any encryption-based algorithms.

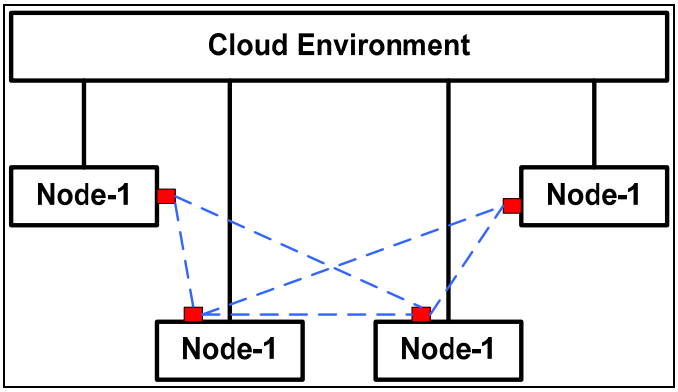


Fig. 2. Cloud Model for Secure Image data propagation

The input image is decomposed into chunks (image data) which are further appended with an encryption security token. Sequential appending and encoding are carried out for the image data over multiple hierarchical layers of the cloud. A typical cloud environment is highlighted in Fig. 2. The core agenda of the proposed model is to present an alternative solution to existing sophisticated encryption algorithms, which have a higher possibility of corrupting the image quality despite better security. Hence, the proposed scheme emphasizes security and retains the image quality to the highest standard. The primary step for this purpose is to construct a secure cloud-based environment where image data can be propagated. A typical environment of a wireless node is constructed as a tree forming an underlying topology connected with a distributed cloud environment. According to Fig.2, there are three different hierarchical layers of the proposed cloud environment. The user base resides on the bottom layer, which interacts with cloud clusters in the second layer for requisitioning image data or reposting them. All the service towards interaction between the user base and cloud cluster is carried out by assigned network devices, e.g., switches, gateways, etc. The cloud network architecture resides in the top layer; this is where the actual algorithm of image security is executed while the responses are forwarded to the user base. As the proposed system uses a cloud environment, the user base is not required to run the actual algorithm (discussed in the next sub-section); however, each user base is programmed to perform a few preliminary operations to ensure security. The cloud-based network considers a large stream where an image is propagated.

5. Mathematical Modeling

The proposed system offers a novel solution for protecting the privacy of the cumulative traffic flow of images. The novelty of the proposed scheme is exhibited in Fig.3, which presents a novel form of an image stream that consists of a digital security code, an encryption token, and image data. Fig. 3 exhibits a unique mechanism of secure indexing to ensure a better form of privacy preservation.

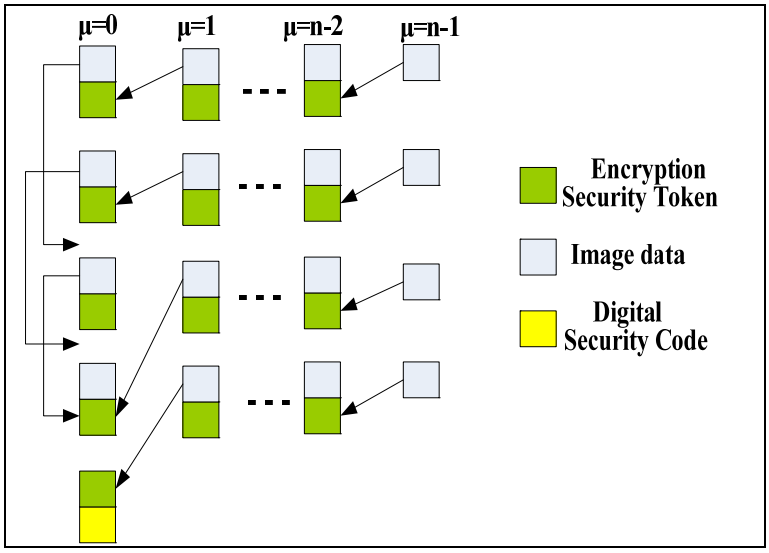


Fig. 3. Mechanism of Privacy Protection in Image

According to this scheme, image data is split into multiple image chunks. The number of splitting of an image is based on the number of carriers allotted for the stream to transmit the image data from the last layer (n-1). In the prior layer (n-2), the image chunk is appended with an encryption token, and the process continues till layer-1. Finally, in layer-0, the image data undergoes a unique transformation. In this scheme, the encryption token for image data residing on any layer with maximum quality is added to the image data of the last layer. This is one of the significant novelties offering dual advantages, viz.

- Owing to the encoding of the image data of the prior layer to encryption token using hashing makes the size of the file smaller and yet retains all the information as meta-data, and
- Due to the appending mechanism of image data and encryption tokens of different sequences and layers, it is nearly impossible even to guess the pattern by any intruder.

For example, as can be seen in Fig. 3, if the encryption token of the 5th image (i=5) data is appended to the 3rd image data (i=3) while the encryption token is appended to image data 0 (i=0) therefore, a predecessor matrix λ_i= (0, 3, 5) will consist of ith image data in 0th layer. For identification of an influence on the privacy preservation operation in the proposed scheme, it is necessary to evaluate the quality of the image for security validation. An empirical expression towards anticipated image quality eI_q is formulated as,

$$eI_q = I_q.A_1 + f_1\left[I_q.\alpha(A_2, A_3)\right].\alpha_\lambda \qquad (1)$$

In the above mathematical expression (1), there is the inclusion of various components. The first component is a product of image quality I_q in the 0th layer and A_1=(1-R_{pe}), where R_{pe} is the packet error rate in the 0th layer. The second component implements a function f_1(x) which is responsible for the summation and product of certain discrete dependable components connecting image quality I_q with the rate of packet errors A_2 and A_3. In a more elaborative form, the function f_1(x) can be discussed in the following form:

$$f_1(x)=(I_q.\ \alpha.A_2)n_0 + (I_q\ .\alpha.A_2)_{\mu.n}x\alpha_\lambda \qquad (2)$$

In the above mathematical expression (2), the first component evaluates a product of image quality I_q and the product of all the rates of packet errors for 0th image data and specific j^{th} layer, where j is a subset of λ_i. The second component evaluates a similar product but considers image quality I_q for a specific layer and product of all rates of packet errors for the ith layer considering all layer information μ and cardinality of image data n. Finally, the variable α_λ states the product of all rates of packet errors (1-R_{pe}) for 0th image data and j^{th} layer. It is also necessary to ensure reduced resource utilization while adopting the proposed privacy preservation scheme. This is necessary to evaluate the degree of computational complexity. Irrespective of various energy computation models both in wireless networks (Setiawan et al. [2018], Ye et al.[2021) and in a cloud environment (Raiker et al.[2021]), they cannot be directly applied owing to the novelty of the proposed scheme which does not match with environment of the existing system. Hence, the proposed scheme constructs very simplified constructs for computing cumulative resource utilization Rs_{cum} while applying the proposed privacy preservation approach as follows:

$$Rs_{cum} = Rs.A_4 + f_2[Rs, \beta, D_{st}, D_h)] \quad (3)$$

In the above mathematical expression (3), the computation of the resource utilization is associated with various dependable variables as follows:

$$A_4 = D_{st} + \beta.D_h + D \quad (4)$$

$$f_2(x) = Rs(\beta.D_h + D) + Rs(D_h + D) + Rs_\mu(D_{\mu-1}) \quad (5)$$

The expression (4) represents the summation of the dimension of security token D_{st} , the product of the redundant channel of hash β for the 0th image data and 0th layer with the dimension of hash D_h, while variable D represents the size of an image. The expression (5) represents another function, $f_2(x)$, which further summates three explicit components. In the above expression, the first component is calculated with respect to n_o-1 layers, while the second component is calculated with respect to (β-2) layers and n_i-1 cardinality of image data. In contrast, the last component is computed with respect to (n_β-1) number of image data considering resources utilized for (β-1) layers and considering the image data dimension of $D_{\mu-1}$. The next part of the implementation is associated with implementing privacy preservation using a computationally cost-effective process. The root image data is appended with the encryption token associated with the 0th layer to increase the privacy preservation degree with a better validation probability, as seen in Figure 3. The mechanism towards allocating the digital security code in the 0th Layer is a progressive process. The prime target of this part of the implementation is to increase the probability of validation $val(\eta)$. The study considers that η for 0th image data and ith image data residing in the 0th layer to be λ_i. Figure 3 exhibits that if the prime encryption token image data is chosen to perform privacy validation of the root node, it uniquely maximizes the validation operation's performance for the image data. This non-iterative process will eventually minimize the probability of performing validation of the privacy attributes stated in expressions (1) and expression (2). For example, if the 5th image data in the 0th layer chooses the prime encryption token image data as its root node, then the system yields $\lambda_5 = \{0, 5\}$. Considering the error rate to be θ for an ith image data with the dimension of D_i, the expression for the probability of validation of privacy can be mathematically represented as follows:

$$val(\eta_{0,5}) = (1-\theta)^{D1}.(1-\theta)^{D2} \quad (6)$$

In the above expression (6), a product of two entities is highlighted, where the variables D_1 and D_2 will represent the summation of D_{st}, D_h, D, and the summation of D_h and D_5, respectively. One important fact to be noted here is that component $(1-\theta)^{D2}$is also inclusive of additional D_h for the newly appended encrypted link of hash data from different layers. In case a different image data is chosen by the 5th data to play the role of root node for validation (say 3rd image data), in such case, the optimal outcome of the predecessor will be $\lambda = \{0,3\}$. Hence, the probability of validation for privacy preservation will always be reduced compared to the prior value. Hence, no extra overhead is added and remains approximately the same throughout the analysis. The strategy mentioned above of the mathematical model is executed in the proposed scheme to offer optimal performance toward privacy preservation. The model controls possible overhead while appending the image data with its hash and encryption token. Further, the novelty of this model is that it is completely independent of any specific form of an intruder. Even if the intruder captures this model by compromising one of some of the wireless devices, it is likely to generate a new encryption token that will never match with others. Finally, the validation fails to result in access deniability by the system. The next section discusses the proposed algorithm implementation.

5.1 Algorithm Implementation

The implementation of the proposed algorithm is carried out considering the underlying methodology discussed in the prior sub-section of mathematical modeling. This section mainly focuses on the mechanism of encryption and decryption to retain a higher degree of privacy in the proposed scheme for any image-based data. The proposed study model is meant to offer privacy for any form of an image, which could carry any privacy construct within it. The only dependency of the proposed implementation is that an integrated development environment should support the conversion of the acquired input image, which is not a challenging task. The algorithm assumes that a wireless node NODE-1 acts as a transmitting node while NODE-2 acts as receiving node. In the entire communication process over a distributed cloud environment, the algorithm primarily emphasizes ensuring the secure transmission of input images. The study also considers the availability of various cloud clusters which store the image chunks in the form of layers, as discussed in the previous section. The first algorithm performs privacy preservation of an image by introducing a very encryption form unlike any existing schemes briefed in Section 2. The operation of the first algorithm is shown in the form of the following algorithmic steps:

Algorithm for Privacy Preservation of Image
Input: I, l_d, μ, n
Output: I_{enc}
Start
1. *init* I, l_d, μ, n
2. **For** i=1:m
3. **For** j=1: μ
4. $c_{bit}=g_1(i, n)$
5. $h_{vec}=g_2(c_{bit})$
6. *alloc* Rs(h_{vec})
7. I_{enc}=forward $[h_{vec}]^{Rs}$
8. **End**
9. **End**
End

The discussion of the internal operation of an algorithm is as follows: The algorithm takes the input of I (input image), l_d (level of decomposition), μ (layers), and n (image chunks in each layer), which undergo series of processing to yield I_{enc} (encrypted image). The proposed scheme considers a mechanism of splitting the image data I into various images with various levels of resolution. The level of decomposition l_d can be assigned by the user based on the size of an image. The proposed scheme considers all the m total number of images on incoming streams (Line-2) and the various number of layers μ (Line-3). A discreet function g_1(x) is constructed, which carry out three series of intrinsic operation as stated below:

- The function g_1(x) obtains a discrete coefficient of the decomposed images i with respect to all the number of images per layer, i.e., n (Line-4). The algorithm obtains multiple coefficients initially for all the decomposed versions of the signal, further decomposed accordingly to the user-specified number of levels. It should be noted that this number of levels l_d is private information that is known only to a specific user. Hence, without this information, no intruder will be unable to initiate the decryption process. Further, all the coefficients are approximated, and their values are determined. Hence, the outcome of the first intrinsic process for g_1(x) is decomposed coefficient with higher resolution.
- The second intrinsic operation carried out by function g_1(x) is to assess all the attributes of an image followed by mapping the respective image attributes in the form of a group of codes/numeric. The prime reason for undertaking this operation by g_1(s) as the secondary process is to generate a standard form of evaluation record towards privacy constructs that can further facilitate the inclusion of the next set of mathematic calculations. This process generates the highest number of co-efficient related to the image chunks concerning user-defined levels of decomposition construct of privacy l_d. The system also generates all the transformed coefficient values with respect to numerical code [0.1 0.8] divided by the compression ratio. Another novelty of this privacy construct is that value of the compression ratio is private information given by the user, which is not anticipated for the intruder to know. The outcome of this internal process is two, i.e., approximated coefficients of all decomposed image chunks and higher values of coefficients of these image chunks.
- The third intrinsic operation carried out by g_1(x) is encoding the symbols by harnessing all the available image chunks that are inversely proportional concerning the symbol probability. The outcome of higher values of coefficient obtained from the secondary intrinsic operation of g_1(x) is considered an input for this third stage of operation to generate communication bits c_{bit} (Line-4). It should be noted that communication bits c_{bit} is formed by considering the hash of the image chunk and approximated coefficient values of image data after both are subjected to these encoding processes.

This algorithm's next line of implementation is towards initiating a secure transmission of the encrypted image based on user-defined layers μ and the number of image data per layer, i.e., n. The study considers $\mu<n$ to facilitate increased propagation of image chunks. The proposed algorithm constructs another discrete function, g_2(x), for this purpose which takes the input argument of recently obtained communication bits c_{bit} from the prior process to yield hash vectors h_{vec} (Line-5). The uniqueness of this process is that it considers all the communication bits c_{bit} obtained to formulate a new entity of image data. This is obtained as follows:

$$chunk_{pp} = \frac{number\ of\ c_{bit}}{\mu.n} \quad (7)$$

In the above expression (7), the image chunk per packet is obtained by dividing the number of communication bits c_{bit} from the product of user-defined layers μ and the number of chunks per layer n. Apart from this, the algorithm applies the one-way hash function to the transposed value of image chunks over c_{bit} to generate hash

vector h_{vec} (Line-5). The next algorithm process is to allocate resources *Rs* using equation (3) over the hash vector h_{vec} (Line-6) towards the assigned communication channel. By performing this step, the algorithm ensures a higher degree of anonymity and privacy towards the assigned communication channel for the secure transmission of image chunks. Finally, the algorithm forwards this hash vector, yielding an arrived encrypted image I_{enc} (Line-7). This completes the algorithmic operation toward performing encryption. The next sequence of algorithm implementation is towards performing decryption. Assuming that the NODE-2 receives the encrypted image data I_{enc}, it is required to perform decryption for this node to access the original transmitted file, i.e., I. This part of the implementation considers that the network has no artifacts while the encrypted data is assumed to be traveled from any normal cloud-based supported network. Hence, this algorithm's prime emphasis is on performing validation of privacy constructs. The steps of the algorithm are stated as follows:

Algorithm for Decryption
Input: I_{enc}, μ, n
Output: I_{dec}
Start
1. For k=1: μ-1
2. **For** l=1:n
3. $h_{rb}=I_{enc}(k, l)$
4. $h_{vr}, I_{str}=h_{rb}$
5. $I_{str}=g_3(I_{str}^T)$
6. $I_{dec}=(h_{vr}, I_{str}^T)$
7. **End**
8. **End**
End

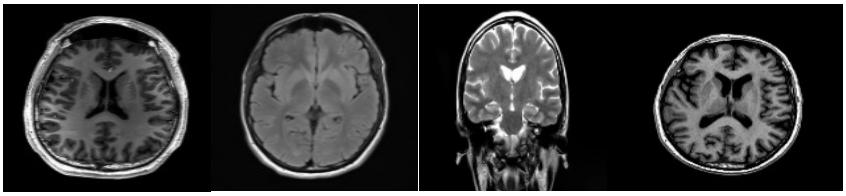
The steps of implementation of the decryption algorithm are as follows: The algorithm takes the input of I_{enc} (Encrypted Image), μ (layers), and n (image chunks in each layer), which finally yields an outcome of I_{dec} (decrypted image). This algorithm assumes that the receiver node NODE-2 is the legitimate node, aware of the values of layer μ and the number of image data per layer used by NODE-1. Any other nodes apart from NODE-1 and NODE-2 do not possess any information related to these privacy constructs. Hence, the receiver node's prime task is to validate the obtained stream of encrypted image data. The operation is considered for residual layers μ-1 (Line-1) and n (Line-2) while the received bits of hashed data h_{rb} matrix are formulated based on selected Ienc suing k and l attribute (Line-3). The proposed algorithm further constructs the received hash vector h_{vr} and the received stream of image data I_{str} by allocating specific rows each for these (Line-4). The third discrete function, g_3(x), is constructed and responsible for carrying out the transposition of the I_{str} (Line-5). Finally, the parameters h_{vr} and transformed value of I_{str} results in decrypted image I_{dec} (Line-6). This completes the decryption operation. Hence, a closer look into the proposed encryption and decryption algorithm shows that it does not carry out any form of the iterative or complex encryption operation, unlike existing approaches. Hence, the proposed algorithm offers cost-effective computational performance and better privacy preservation against various lethal threats to images. The next section discusses the results of implementing the proposed scheme.

6. Result

As the proposed scheme emphasizes securing different forms of an image, a specific set of environments is required to testify to this. Apart from this, as the proposed scheme mainly uses image data and chunks obtained from it along with its transformation towards hash and digital security code, it is essential to realize if such a form of generated images is practical enough to be executed. Further, as the proposed system introduces a novel encryption scheme, which is very different from any conventional image cryptographic scheme, it is essential to assess its computational performance to support the security objectives towards privacy preservation.

6.1 Simulation Environment

The discussion of the scheme is carried out with a standard dataset. The complete implementation of the proposed scheme is carried out in a MATLAB environment using a normal 64-bit windows machine with 16GB RAM. The simulation environment involves developing a user interface, which the transmitting node uses over a wireless environment to upload the image into a cloud-distributed storage unit. The study considers the adoption of standard IEEE 802.11 deployed within each wireless node, which requires applying the first encryption algorithm towards propagating the file upon acquiring the image file. Apart from the network environment, adopting an image dataset is essential in analyzing the result.



(a) Sample of Brain MRI dataset [Chakrabarty, N., 2019]

(b) Sample of satellite image dataset [Reda, M. 2021]

(c) Sample of traffic scene image dataset [Multimedia Laboratory]

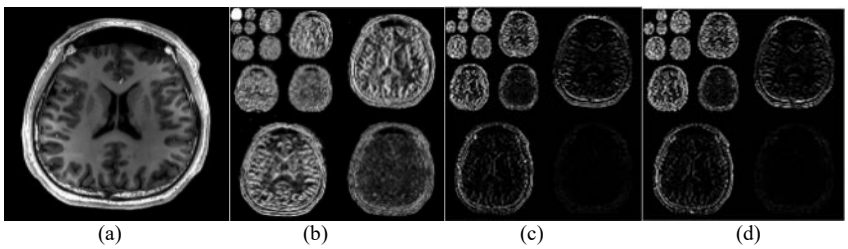
(d) Frequently used Image dataset [Wang, Y., Smaple Images]

Fig.4. Visuals of the Image Dataset Experimented

Fig. 4 highlights the sample visuals of various image datasets for analyzing the proposed study model. The proposed system considers multiple sets of images from different datasets that are publicly available. The proposed scheme has been analyzed with different image datasets to evaluate its performance consistency. Approximately 5000 images were assessed in this evaluation process, which ensured that the study model could process an input image irrespective of any type, format, size, and memory of images. However, the format supportability is restricted to JPEG, PNG, TIFF, BMP, and DICOM only, as MATLAB offers supportability towards specific formats only. However, it is never a bigger concern as most publicly available datasets come under the aforementioned formats. This next section highlights the outcome obtained during the experiment.

6.2 Outcome Accomplished

The outcome accomplished in the study is presented in the form of visual and graphical outcomes for better representation in practical form. Exhibiting the visual outcomes for 5000 images is out of the scope of this paper, and hence a sample use case of outcomes of the brain MRI dataset is presented in this section. Fig. 5(a) showcases the original input brain MRI image, which upon decomposition, exhibits the decomposed version of the outcome as shown in Fig. 5(b). The three internal operations of function g1(x) are showcased in Fig. 5(b), Fig. 5(c), and Fig. 5(d). Fig. 6 represents the sequence of generation of the encrypted image, where Fig. 6(a) represents the generated hash vector h_{vec}. In contrast, Fig. 6(b) represents the allocated resources Rs for transmitting encrypted image I_{enc}.



(a) (b) (c) (d)

Fig. 5. Visual outcome processing of brain MRI

d0754444d0...	9a4468c1f8...	04d55b1ff42...	43b97b767d...	a6e0485a39...	0c8954aa34...
584b868e6f...	8b5260c7fb...	a0bdd019cd...	f9478e59d5...	0a306d5b61...	0c8139a946...
8284de3092...	75b0413aee...	6b16d6aa5b...	8e06c53362...	53464b5ef6...	88674c61cc...
be4c9e8eb3...	6073d1a78a...	6030b44548...	130daf31ebf...	24b71da239...	582d0a6b1f...
e338f67f8b2...	9caa415890...	0f9dde59f25...	9eafe187e0...	dd7464a810...	6a93908c0d...
07b581435e...	11c82193c9...	7dc8b4ecc9...	2ba7047f50...	d66a28d98a...	9280c95394...
0d11d7c033...	f6b66e044c...	c2cdd2b94f...	e8b288eece...	1aff2f24ecc...	e2da3ca36c...
c05a1e5ea3...	9134070d8e...	29fa250471...	483ecd0b9b...	2779039e6a...	f55a7be30d...
2b10f1c00b...	916f35ef279...	a3970af1d6...	57f2981d6fd...	25a6eecca8...	8abb605b43...
0055b64280...	7a02572f36...	82947c9978...	0aeda1b873...	488db40b6a...	bd92c33416...

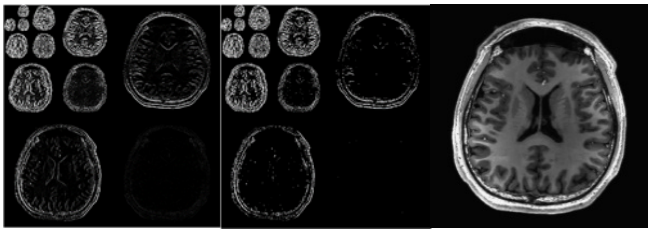
(a)

584b868e6f...	8b5260c7fb...	a0bdd019cd...	f9478e59d5...	0a306d5b61...	0c8139a946...
8284de3092...	75b0413aee...	6b16d6aa5b...	8e06c53362...	53464b5ef6...	88674c61cc...
be4c9e8eb3...	6073d1a78a...	6030b44548...	130daf31ebf...	24b71da239...	582d0a6b1f...
e338f67f8b2...	9caa415890...	0f9dde59f25...	9eafe187e0...	dd7464a810...	6a93908c0d...
07b581435e...	11c82193c9...	7dc8b4ecc9...	2ba7047f50...	d66a28d98a...	9280c95394...
0d11d7c033...	f6b66e044c...	c2cdd2b94f...	e8b288eece...	1aff2f24ecc...	e2da3ca36c...
c05a1e5ea3...	9134070d8e...	29fa250471...	483ecd0b9b...	2779039e6a...	f55a7be30d...
2b10f1c00b...	916f35ef279...	a3970af1d6...	57f2981d6fd...	25a6eecca8...	8abb605b43...
0055b64280...	7a02572f36...	82947c9978...	0aeda1b873...	488db40b6a...	bd92c33416...
0100000000...	0010010011...	0111100111...	0100101100...	1101000101...	0000000001...

(b)

Fig. 6. Generation of Encrypted Image data

A closer look into the hash values between Fig. 6(a) and Fig. 6(b) shows that each cell consists of different values between themselves, which will eventually mean the transformation process of the encrypted values in each progressive step. This operation also exhibits better retention of forward secrecy maintained in the proposed encryption algorithm. Finally, the encrypted image is transmitted to the wireless channel of IEEE 802.11 standard, where the receiver obtains the encrypted image and initiates the decryption process.



(a) (b) (c)

Fig. 7. Arrival of Decrypted Image

The visuals of the decryption operation are exhibited in Fig. 7. After acquiring the encrypted image by the receiver node, it performs validation of the hash vector. Fig. 7(a) highlights the outcome of acquiring the decomposed coefficient of hash vectors. In contrast, Fig. 7(b) represents inversing the second intrinsic operation carried out by the $g_1(x)$ function, which upon applying the $g_3(x)$ function, offers an outcome of the decrypted image as per the second algorithm. The next part of the result analysis is based on graphical outcomes, where a comparative analysis is carried out. For benchmarking, the proposed scheme (Prop) is compared with the frequently reported scheme of image privacy preservation, viz. Homomorphic Encryption HomEnc [Bi *et al.*, 2022]; [Yang *et al.*, 2020]; [Yang *et al.*, 2018], Deep Learning Based Encryption (DLBE) [Alkhelaiwi *et al.*, 2021]; [Huang *et al.*, 2022], Blockchain Based Management (BCM) [Zerka *et al.*, 2020], Key-Based Encryption (KBE) [Sheidani *et al.*, 2021]. The proposed scheme considers an extensive test bed to carry out this analysis.

6.3 Comparative Analysis

All the graphical analysis is carried out with an increasing score of compression ratio. The justification behind this assumption is that as the proposed scheme works on a wireless network environment over a cloud interface, it is more likely that compression will be carried out over images with variable sizes. Hence, with an increased compression ratio, it is anticipated to assess the better retention of target performance parameters in the y-axis of each graph. The first performance parameter considered for analysis is a resolution computed as bits per pixel (bpp). Resolution is an essential parameter while applying an encryption algorithm to assess the decrypted image's outcome. The outcome shown in Fig. 8 highlights that the proposed system offers better retention of resolution in contrast to all other existing schemes. Applying Key-Based Encryption (KBE) has higher dependencies on the computation of secret keys and extracted features. The adoption of high-level features leads to a significant declination of resolution.

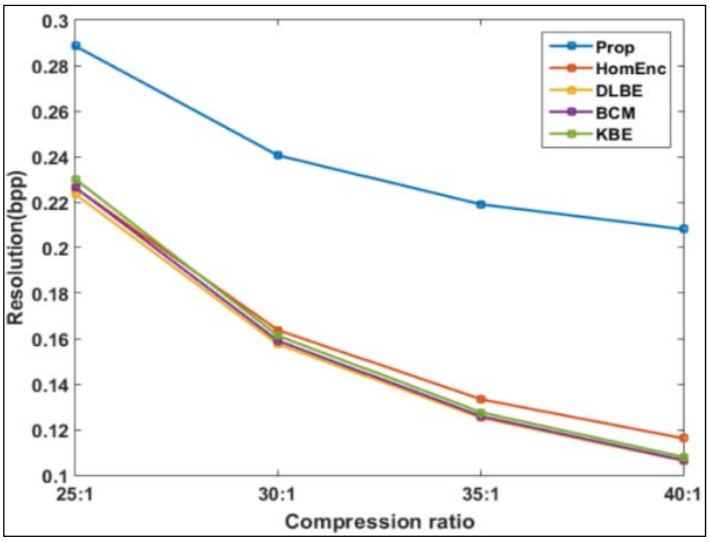


Fig. 8. Comparative Analysis of Resolution

The adoption of blockchain offers significant security and performs well during encryption. However, the complex form of image pixels is not acquired during decryption. The process runs well for static images but not for a stream of images. The adoption of deep learning offers a higher degree of security solution, but with the inclusion of massive iterative operational steps, the resolution potentially degrades. Applying homomorphic encryption converts the complete image into ciphertext, which is good from a security viewpoint but also leads to poor performance during decryption, especially for larger images. The prime reason for the better resolution of the proposed system is due to the interconnection of image chunks with hash in the form of hash vectors, which retain complete information without losing any significant pixel of information. The next round of assessment is associated with image quality defined in the form of peak signal-to-noise ratio. Figure 9 exhibits a stiff drop in image quality with an increased compression ratio, which is quite normal in peak traffic conditions. However, the contribution of this outcome is that the proposed scheme offers comparatively better image quality than other existing privacy preservation techniques reported in the existing scheme. A similar justification for resolution is also applicable to the outcome of image quality in Fig. 9.

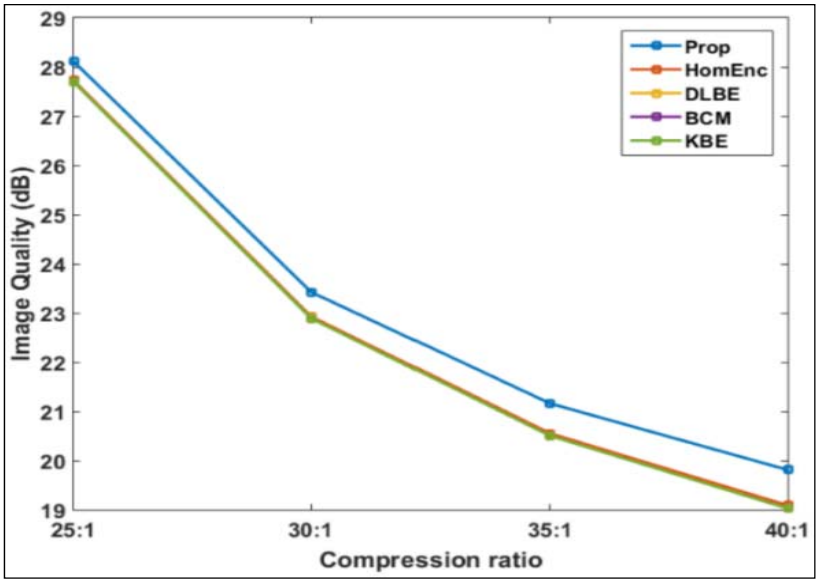


Fig. 9. Comparative Analysis of Image Quality

The final performance parameter evaluated is overhead. As the proposed scheme permits linking hash with the image data in different layers, the possibility of overhead must be assessed. As per expression (6) in the previous section, the proposed scheme offers a significant control of overhead using a series of mathematical operations. However, there is no explicit module for overhead control in any of the reported schemes of the existing system. Therefore, the outcome exhibited in Fig.10 offers better results for the proposed scheme.

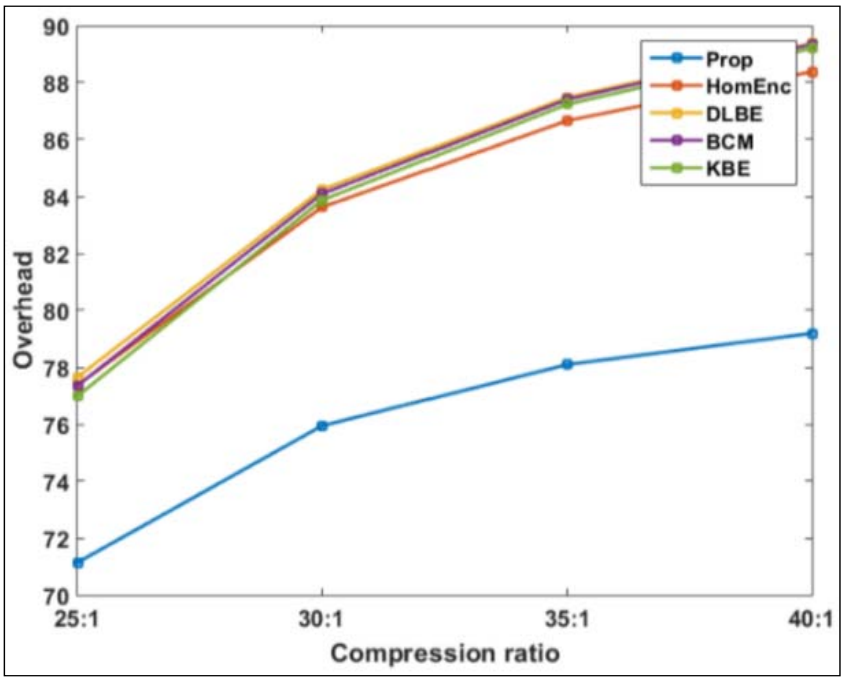


Fig. 10. Comparative Analysis of Overhead

Another reason for better overhead performance in contrast to the existing scheme is a higher inclination of iterative and sophisticated computational processes in existing studies.

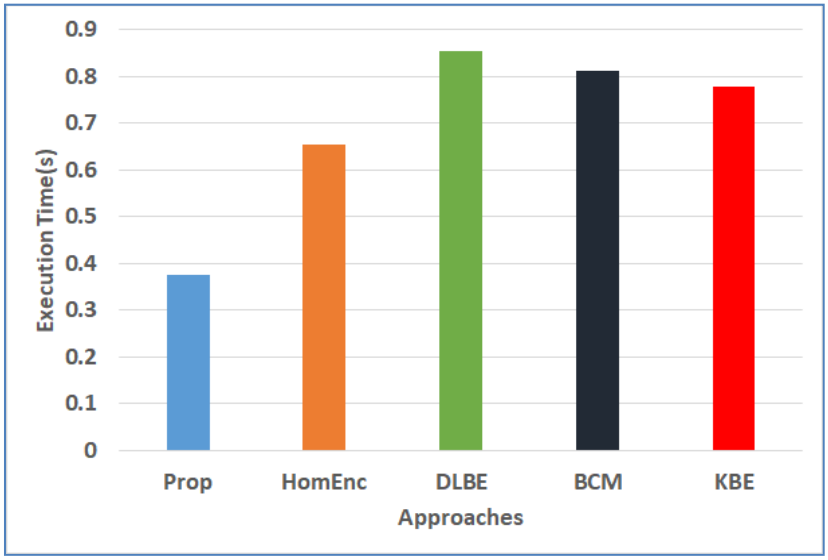


Fig. 11. Comparative Analysis of Execution Time

Management of hash vectors using a secured hash algorithm and one-way hash function offers better performance scalability and consistency. Hence, the proposed scheme offers better privacy preservation performance. Finally, the execution time for the proposed system is found to be quite lesser compared to all the existing approaches for a similar reason stated in prior graphical outcomes. The outcome quantification exhibits proposed system offers approximately 40% reduced execution time over the increased iteration range [0-500] in contrast to average values of the execution time of existing schemes.

6.4 Discussion and limitation

From the previous section, it is noted that proposed system offers significantly lesser execution time in contrast to other existing approaches. Apart from this, proposed scheme also offers reduced overhead, higher image quality, and better resolution over increasing compression ratio when assessed over similar test-bed with existing

scheme being analyzed too. The justification behind the better form of outcomes for proposed system is also stated in prior section. However, there is further limitation too as follows:

- The proposed scheme can suitably resist any form of key-based attack; however, it is not analyzed for pure node capture attack.
- The core data that is subjected for security operations in proposed system is mainly image file and outcomes offer justifiable security accomplishment. However, the scheme is not meant to support multimedia application like securing video files.
- The complete modeling is carried out considering heterogeneous and complex form of attackers. However, the initiation of attack is singular form and the model cannot resists any event of concurrent multi-attacker

7. Conclusion and Future Work

The proposed study presents an integrated framework that can retain maximum privacy preservation over different types of images. The novelty of contribution of the proposed scheme are as follows: i) the proposed scheme facilitates encryption for complete stream of images unlike the existing schemes which considers securing single images only, ii) the mathematical modelling presented in the paper can compute the necessary resources to be used for supporting the privacy constructs as well as it can also validate the genuineness of the image, iii) the scheme can control potential overhead even after linking various hash vectors with image chunks of next layer, iv) the scheme offers multiple layer of security and untrace-ability of the hash vectors even if it is compromised by an intruder, v) The quality of an image is well maintained in the entire course of encryption which is highly supportive of retention of private details from application perspective, vi) The quantified outcome of proposed scheme shows that it offer approximately 65% of better resolution, 25% of better PSNR, and 59% of reduced overhead compared to existing techniques. Our future work direction will be toward further optimizing the encryption process. The possible shortcoming of the proposed scheme could be that it is not designed to consider node capture attack, which is an irreversible form of physical attack. Apart from this, the model is highly resistant to most attacks and offers higher privacy without affecting communication performance. Future work could be carried out toward further inclusion of optimization concepts for leveraging encryption techniques. Future work could also be directed toward assessing the impact of concurrent multi-attacker over similar transmission regions.

Funding

No funding is provided for the preparation of manuscript.

Conflicts of interest

The authors have no conflicts of interest to declare

References

[1] Alkhelaiwi, M., Boulila, W., Ahmad, J., Koubaa, A., & Driss, M. (2021). An efficient approach based on privacy-preserving deep learning for satellite image classification. *Remote Sensing*, *13*(11), 2221. doi:10.3390/rs13112221

[2] Bi, X., Shuai, C., Liu, B., Xiao, B., Li, W., & Gao, X. (2022). Privacy-preserving color image feature extraction by quaternion discrete orthogonal moments. *IEEE Transactions on Information Forensics and Security*, *17*, 1655–1668. doi:10.1109/tifs.2022.3170268

[3] Boulemtafes, A., Derhab, A., & Challal, Y. (2020). A review of privacy-preserving techniques for deep learning. *Neurocomputing*, *384*, 21–45. doi:10.1016/j.neucom.2019.11.041.hal-02921443

[4] Cai, G., Wei, X., & Li, Y. (2022). Privacy-preserving CNN feature extraction and retrieval over medical images. *International Journal of Intelligent Systems*, *37*(11), 9267–9289. doi:10.1002/int.22991

[5] Chai, X., Wang, Y., Gan, Z., Chen, X., & Zhang, Y. (2022). Preserving privacy while revealing thumbnail for content-based encrypted image retrieval in the cloud. *Information Sciences*, *604*, 115–141. doi:10.1016/j.ins.2022.05.008

[6] Chakrabarty, N. (2019, April 14). Brain MRI images for Brain tumor detection. Retrieved February 14, 2023, from https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection

[7] Chen, Z., Zhu, T., Wang, C., Ren, W., & Xiong, P. (2020). GAN-based image privacy preservation: Balancing privacy and utility. In *Machine Learning for Cyber Security* (pp. 287–296). Cham: Springer International Publishing.

[8] Cheng, H., Huang, Q., Chen, F., Wang, M., & Yan, W. (2022). Privacy-preserving image watermark embedding method based on edge computing. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 18570–18582. doi:10.1109/access.2022.3151115

[9] Cunha, M., Mendes, R., & Vilela, J. P. (2021). A survey of privacy-preserving mechanisms for heterogeneous data types. *Computer Science Review*, *41*(100403), 100403. doi:10.1016/j.cosrev.2021.100403

[10] Debnath, B., Das, J. C., De, D., Mondal, S. P., Ahmadian, A., Salimi, M., & Ferrara, M. (2020). Security analysis with novel image masking-based quantum-dot cellular automata information security model. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 117159–117172. doi:10.1109/access.2020.3002081

[11] Deng, T., Li, X., Jin, B., Chen, L., & Lin, J. (2021). Achieving lightweight privacy-preserving image sharing and illegal distributor detection in social IoT. *Security and Communication Networks*, *2021*, 1–13. doi:10.1155/2021/5519558

[12] Guo, C., Jia, J., Choo, K.-K. R., & Jie, Y. (2020). Privacy-preserving image search (PPIS): Secure classification and searching using convolutional neural network over large-scale encrypted medical images. *Computers & Security*, *99*(102021), 102021. doi:10.1016/j.cose.2020.102021

[13] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.-H. A., Habib, S., … Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 47731–47742. doi:10.1109/access.2021.3061710
[14] Hassanpour, A., Moradikia, M., Yang, B., Abdelhadi, A., Busch, C., & Fierrez, J. (2022). Differential privacy preservation in robust continual learning. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 24273–24287. doi:10.1109/access.2022.3154826
[15] Huang, Q.-X., Yap, W. L., Chiu, M.-Y., & Sun, H.-M. (2022). Privacy-preserving deep learning with learnable image encryption on medical images. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 66345–66355. doi:10.1109/access.2022.3185206
[16] Iida, K., & Kiya, H. (2020). Privacy-preserving content-based image retrieval using compressible encrypted images. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 200038–200050. doi:10.1109/access.2020.3035563
[17] Ito, H., Kinoshita, Y., Aprilpyone, M., & Kiya, H. (2021). Image to perturbation: An image transformation network for generating visually protected images for privacy-preserving deep neural networks. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 64629–64638. doi:10.1109/access.2021.3074968
[18] Janani, T., & Brindha, M. (2022). SEcure similar image matching (SESIM): An improved privacy preserving image retrieval protocol over encrypted cloud database. *IEEE Transactions on Multimedia*, *24*, 3794–3806. doi:10.1109/tmm.2021.3107681
[19] Jiang, L., Xu, C., Wang, X., Luo, B., & Wang, H. (2020). Secure outsourcing SIFT: Efficient and privacy-preserving image feature extraction in the encrypted domain. *IEEE Transactions on Dependable and Secure Computing*, *17*(1), 179–193. doi:10.1109/tdsc.2017.2751476
[20] Jiao, S., Lei, T., Gao, Y., Xie, Z., & Yuan, X. (2019). Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 119557–119565. doi:10.1109/access.2019.2936119
[21] Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 37855–37865. doi:10.1109/access.2021.3063237
[22] Kiya, H., Nagamori, T., Imaizumi, S., & Shiota, S. (2022). Privacy-preserving semantic segmentation using vision transformer. *Journal of Imaging*, *8*(9), 233. doi:10.3390/jimaging8090233
[23] Ko, D.-H., Choi, S.-H., Shin, J.-M., Liu, P., & Choi, Y.-H. (2020). Structural image DE-identification for privacy-preserving deep learning. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 119848–119862. doi:10.1109/access.2020.3005911
[24] Li, T., Qiu, Z., Cao, L., Cheng, D., Wang, W., Shi, X., & Wang, Y. (2021). Privacy-preserving participant grouping for mobile social sensing over edge clouds. *IEEE Transactions on Network Science and Engineering*, *8*(2), 865–880. doi:10.1109/tnse.2020.3020159
[25] Liu, C., Zhu, T., Zhang, J., & Zhou, W. (2023). Privacy intelligence: A survey on image privacy in online social networks. *ACM Computing Surveys*, *55*(8), 1–35. doi:10.1145/3547299
[26] Ma, X., Ma, J., Li, H., Jiang, Q., & Gao, S. (2021). PDLM: Privacy-preserving deep learning model on cloud with multiple keys. *IEEE Transactions on Services Computing*, *14*(4), 1251–1263. doi:10.1109/tsc.2018.2868750
[27] Mohanty, M., Zhang, M., Asghar, M. R., & Russello, G. (2021). E-PRNU: Encrypted domain PRNU-based camera attribution for preserving privacy. *IEEE Transactions on Dependable and Secure Computing*, *18*(1), 426–437. doi:10.1109/tdsc.2019.2892448
[28] Multimedia Laboratory. (n.d.). Multimedia laboratory. Retrieved February 14, 2023, from Edu.hk website: http://mmlab.ie.cuhk.edu.hk/datasets/mit_traffic/index.html
[29] Nakamura, K., Nitta, N., & Babaguchi, N. (2019). Encryption-free framework of privacy-preserving image recognition for photo-based information services. *IEEE Transactions on Information Forensics and Security*, *14*(5), 1264–1279. doi:10.1109/tifs.2018.2876752
[30] Puteaux, P., & Puech, W. (2021). CFB-then-ECB mode-based image encryption for an efficient correction of noisy encrypted images. *IEEE Transactions on Circuits and Systems for Video Technology: A Publication of the Circuits and Systems Society*, *31*(9), 3338–3351. doi:10.1109/tcsvt.2020.3039112
[31] Raiker, G. A., Reddy B., S., Loganathan, U., Agrawal, S., Thakur, A. S., Ashwin, … Thomson, M. (2021). Energy disaggregation using energy demand model and IoT-based control. *IEEE Transactions on Industry Applications*, *57*(2), 1746–1754. doi:10.1109/tia.2020.3047016
[32] Raynal, M., Achanta, R., & Humbert, M. (2020). Image obfuscation for privacy-preserving machine learning. Retrieved from http://arxiv.org/abs/2010.10139
[33] Reda, M. (2021). *Satellite Image Classification* [Data set]. Retrieved February 14, 2023, from https://www.kaggle.com/datasets/mahmoudreda55/satellite-image-classification
[34] Setiawan, D., Aziz, A. A., Kim, D. I., & Choi, K. W. (2018). Experiment, modeling, and analysis of wireless-powered sensor network for energy neutral power management. *IEEE Systems Journal*, *12*(4), 3381–3392. doi:10.1109/jsyst.2017.2774285
[35] Sheidani, S., Mahmoudi-Aznaveh, A., & Eslami, Z. (2021). CPA-secure privacy-preserving reversible data hiding for JPEG images. *IEEE Transactions on Information Forensics and Security*, *16*, 3647–3661. doi:10.1109/tifs.2021.3080497
[36] Sirichotedumrong, W., Kinoshita, Y., & Kiya, H. (2019). Pixel-based image encryption without key management for privacy-preserving deep neural networks. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 177844–177855. doi:10.1109/access.2019.2959017
[37] Sun, X., Tian, C., Tian, W., & Zhang, Y. (2022). Privacy-enhanced and verifiable compressed sensing reconstruction for medical image processing on the cloud. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 18134–18145. doi:10.1109/access.2022.3151398
[38] Wang, Y. (n.d.). Sample images. Retrieved February 14, 2023, from Nyu.edu website: https://eeweb.engineering.nyu.edu/~yao/EL5123/SampleData.html
[39] Yang, H., Zhou, Q., Ni, J., Li, H., & Shen, X. (2020). Accurate image-based pedestrian detection with privacy preservation. *IEEE Transactions on Vehicular Technology*, *69*(12), 14494–14509. doi:10.1109/tvt.2020.3043203
[40] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 131723–131740. doi:10.1109/access.2020.3009876
[41] Yang, T., Ma, J., Wang, Q., Miao, Y., Wang, X., & Meng, Q. (2018). Image feature extraction in encrypted domain with privacy-preserving Hahn moments. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 47521–47534. doi:10.1109/access.2018.2866861
[42] Yang, Y., Xiao, X., Cai, X., & Zhang, W. (2020). A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images. *IEEE Signal Processing Letters*, *27*, 256–260. doi:10.1109/lsp.2020.2965826
[43] Ye, H.-T., Kang, X., Joung, J., & Liang, Y.-C. (2021). Optimization for wireless-powered IoT networks enabled by an energy-limited UAV under practical energy consumption model. *IEEE Wireless Communications Letters*, *10*(3), 567–571. doi:10.1109/lwc.2020.3038079
[44] Yi, F., Jeong, O., & Moon, I. (2021). Privacy-preserving image classification with deep learning and double random phase encoding. *IEEE Access: Practical Innovations, Open Solutions*, *9*, 136126–136134. doi:10.1109/access.2021.3116876
[45] Zerka, F. (2020). Blockchain for Privacy Preserving and Trustworthy Distributed Machine Learning in Multicentric Medical Imaging (C-DistriM). *IEEE Access*, *8*, 183939–183951. doi:10.1109/ACCESS.2020.3029445.T
[46] Zhang, L., Jung, T., Liu, K., Li, X.-Y., Ding, X., Gu, J., & Liu, Y. (2017). PIC: Enable large-scale privacy preserving content-based image search on cloud. *IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society*, *28*(11), 3258–3271. doi:10.1109/tpds.2017.2712148

[47] Zhang, Z., Cilloni, T., Walter, C., & Fleming, C. (2021). Multi-scale, class-generic, privacy-preserving video. *Electronics*, *10*(10), 1172. doi:10.3390/electronics10101172
[48] Zheng, M., Xu, D., Jiang, L., Gu, C., Tan, R., & Cheng, P. (2019). Challenges of privacy-preserving machine learning in IoT. Retrieved from http://arxiv.org/abs/1909.09804
[49] Zheng, Y., Duan, H., Tang, X., Wang, C., & Zhou, J. (2021). Denoising in the dark: Privacy-preserving deep neural network-based image denoising. *IEEE Transactions on Dependable and Secure Computing*, *18*(3), 1261–1275. doi:10.1109/tdsc.2019.2907081
[50] Zhou, F., Qin, S., Hou, R., & Zhang, Z. (2022). Privacy-preserving image retrieval in a distributed environment. *International Journal of Intelligent Systems*, *37*(10), 7478–7501. doi:10.1002/int.22890
[51] Zhou, J., Li, J., & Di, X. (2020). A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 122210–122228. doi:10.1109/access.2020.3007550

Authors Profile

Chhaya S Dule is presently working in the department of computer science and engineering , Dayananda Sagar University Bangalore , Karnataka ,India.She is pursuing Ph.D in Computer Science and Engineering, from Visvesvaraya Technological University, Belgaum. She has completed B.E and M.Tech from reputed institutions. She is having 23+ years of teaching experience. Her domain area of research is High Performance Computing ,Cloud Computing, Security issues in cloud computing . Her other area of research interest are DBMS, , Big Data Analytics , Data Mining and Data Warehousing , Neural Network, Fuzzy logic.She has also served as Head of the Department. She is coordinator for NBA and NAAC accreditation process. She has research publications in reputed National and International scopus indexed journals. She has attended 4 faculty development programs (FDP) organized by AICTE and TEQIP and 8 workshops on various topics. She has organized various Faculty Development Programs. She has guided UG/PG various projects. She is Life Member of CSI and ISTE professional bodies

Dr. Roopashree HR has completed B.E(E&C) and M.Tech(CS&E) from VTU Belagavi, Karnataka ,India and PhD from Christ University (Deemed to be University) Bengaluru ,Karnataka .She has around 13 years of Industrial experience and 3 years of teaching experience. She is presently working as Associate professor in the department of Computer Science and Engineering at GSSSIETW, Mysuru, India and supervising 6 PhD research scholars in VTU.