Journal of Biological Regulators and Homeostatic Agents 2025, 39(4), 8284.
https://doi.org/10.54517/jbrha8284

Article

Extracting image features with data integrity and confidentiality by verifiable outsourcing computation in cloud computing

Sivakumar Kumaresan[1,*], Golden Julie Eanoch[2]

[1] Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu 627003, India
[2] Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, Tamil Nadu 627007, India
*** Corresponding author:** Sivakumar Kumaresan, sivakumar.francis@outlook.com

CITATION

Kumaresan S, Eanoch GJ. Extracting image features with data integrity and confidentiality by verifiable outsourcing computation in cloud computing. Journal of Biological Regulators and Homeostatic Agents. 2025; 39(4): 8284. https://doi.org/10.54517/jbrha8284

ARTICLE INFO

Received: 27 Qctober 2025
Revised: 3 November 2025
Accepted: 5 November 2025
Available online: 6 January 2026

Abstract: Due to rapid enhancement of digital communication in cloud paradigm, easier transmission & storage of the multimedia information in several platforms becomes challenging. The security of image information is vital since the images are considered as a major component of communication in cloud environment. The secret information is shared in the form of secured image which needs to be retrieved and send to user without losing the integrity and confidentiality of data. For this purpose, the proposed model is designed which employs feature extraction categorization process and transmitting extracted information securely via cryptographic process. Initially the input images are retrieved and parameter initialization is carried by bilinear matrix. An optimal feature extraction is carried using Rotational invariant Local Binary Pattern (RI-LBP) along with Enriched Shark smell optimization process for extracting features of secret information. E-IBE (Enhanced-Identity based encryption) is employed for private key generation followed by cryptographic process via Ensemble Improved Homomorphic Pailler and Quantized ElGammal Elliptic curve Cryptography (ECC) scheme. The decrypted outcome attained is then digitally verified by employing SHA3 verification model. Thus, retrieved data is provided to the user after validation in a secured manner. The simulation results are then observed by analyzing the proposed scheme performance on CIFAR-10 dataset &MNIST dataset attained outcomes are compared with traditional schemes to validate the enhancement of proposed model over other models. the performance is carried for various metrics like extraction accuracy, recall, precision F1-score, precision-recall curve, RoC curve, execution time, runtime & storage space of entire system.

Keywords: cloud paradigm; image security; secured transmission of secret image; image feature extraction; private key generation; cryptographic scheme; SHA3 digital verification

1. Introduction

In the modern digital era, images on electronic devices or any sort of computing device are growing, such as story-sharing platforms like Facebook, Twitter, hospital management system (HMS) records, and secure military records, where a greater number of images are stored and accessed. To analyze these images in a secure and safe way, some advanced techniques need to be implemented to achieve CIA traits. To ensure the integrity and confidentiality of accessing the images, some security techniques, like cryptanalysis, are to be processed to prevent unauthorized access to images on any cloud platform. To propose advanced techniques to extract images in a secure way under a cloud platform and standalone devices to protect user sensitive data without any loss or masquerade. Images are used in a public access and private process in accessing data such as each individual user has account to access their images and Hospital management system scan report need privacy to protect sensitive data of the user and the organizations, other than this some military access data also very different to process in a military grade authentication to access all data by particular user if the integrity is loss in the accessing method means our data will create huge personal loss to the every single user makes this security in imaging system as a challenging task to protect images not cracked by the unauthorized person our proposed model use advanced security techniques to prevent images from the unauthorized access extracted in a safe way to recover from its original state in a safe and secure cryptanalysis method [1,2].

Virtual storage environments in the domain of cloud computing have evolved massively over the past year, storing numerous numbers of bits and bytes of data in cloud resources and accessing the data anytime, anywhere, creating more flexibility for the user. Relatively relying on centralized, costly to establish, manage, and run traditional data centers, cloud computing offers remote access to an endless supply of resources that are made available over the internet whenever needed. While there are many benefits to cloud computing, such as cost savings, scalability, and elasticity, there are also significant cybersecurity dangers. They specifically demand the integrity of the data and computations, which means that the data and results should stay valid even in the event that the cloud servers are compromised, and end-to-end confidentiality of the data, which means that the data should remain secret from Cloud Services Providers (CSPs). Governmental organizations, for instance, purchase cloud services contingent upon meeting certain requirements and being recognized as a reliable source of secure services [3]. Despite the time-consuming and expensive procedures involved in satisfying these standards, no mathematically sound guarantees on the security of data and computation can be made. In this work, we seek to utilize readily accessible commercial CSPs independently of their security protocols or dependability.

The advent of big data has come about as a result of technical breakthroughs. Network popularity has increased dramatically, information interaction technology has evolved, and computer and internet technology have progressed quickly. Even though the majority of people use the Internet to transfer information, there are numerous hazards to data security. As networks spread into new sectors, data transmission security is having a rapid impact on people’s security as well as that of companies and even entire nations. An image has a powerful expressive influence on the data it contains due to its visual characteristics. Due to their extensive use in information interaction, images are preferred in many information expressions. Valuable photo owners regularly use the Internet to post their image data or hold auctions. This method not only saves money but also eliminates geographical restrictions like geography and is quick and convenient [4]. However, vulnerable picture data components offer a window of opportunity for malicious assaults throughout the network transmission process. As a result, original image data may be compromised, leading to data loss or corruption. Enhancing the security of image data, lowering the possibility of data loss or destruction, and guaranteeing the safe transfer of original data are the objectives of picture encryption. Data theft and other forms of malicious attack are frequent, and picture encryption technology is always developing.

Enhancing the image security, key transmission security, and anti-attack capability is an essential issue that needs to be addressed [5-7].

Two fundamental problems in contemporary computer vision systems are feature extraction and segmentation, which taken together form the system's core. Feature extraction is a process used in machine learning, pattern recognition, and image processing that starts with an initial set of measurement data and creates derived values (features) with the goal of offering information and non-redundancy [8]. This makes the subsequent learning and generalization stages easier to complete and, in certain situations, improves interpretability. The process of extracting an image's local structure, content features, and global features is known as image feature extraction. Complex images can have their essential features with significant data content, high repeatability, and distinguishability extracted by feature extraction [9]. The classic picture feature extraction techniques are based on three primary approaches: knowledge-based, artificial neural network-based, and statistical model-based. Since the 1980s, artificial neural networks have been the focus of much study in the field of artificial intelligence [10-14]. In order to create a basic model, it abstracts the neural network of the human brain from the standpoint of information processing and creates several networks based on various connection patterns. The first two techniques are a bit more advanced. But the majority of these techniques are theoretical in nature. These approaches don't seem to be sufficient for the segmentation problem in images. As a result, numerous academics have put forth various improved algorithms based on the evaluation of earlier work.

The main contribution of the paper is:

- The main highlight of this research is to process an image processing paradigm that incorporates the extraction of characteristics from input photos and their secure storage, in addition to authorized cloud storage.
- The method proposed here optimization is carried using Enriched Shark smell optimization, and private key generation takes place using E-IBE (Enhanced-Identity based encryption).
- To achieve hybrid cryptographic process is carried using Ensemble Improved Homomorphic Pailler and RSA Cryptography scheme so as to make encryption and decryption whose decrypted output is verified with the MD5 function
- Initially the input images are updated and parameter initialization is carried by bilinear matrix. The feature extraction is carried from the input image by means of employing optimization and Rotational invariant LBP based feature extraction so as to extract secret information's feature.
- The final results observed to analyze the performance of proposed scheme and compared with other traditional models.

The paper is structured as follows: Section II discusses the literatures related to image feature extraction and security approaches. Section III described the proposed methodologies and materials for the image feature extraction and secure storage in cloud. Section IV discusses the experimented results with comparison. Section V concludes the proposed model results with its merits, demerits and future extension.

2. Related works

This section discusses the related literatures of image feature extraction and secure storage in cloud with integrity and confidentiality. In order to extract image features Xu et al. [6] presented a model based on visual information. The outcomes demonstrated that, under identical conditions, the feature extraction time of the X method for various targets was within 0.5 s. With a correct matching rate of over 90%, the feature matching time was within 1 s. For various targets, the Y algorithm's time for feature extraction was under two seconds. The X algorithm had a superior recognition effect compared to the Y method, as evidenced by the feature matching time of less than 3 s and the correct matching rate ranging from 80 to 90%. It shows that the image feature extraction algorithm and visual information have a beneficial association [7].

Yang et al. [15] interested in the issue of effective data integrity auditing that facilitates verifiable data updates in cloud computing environments. Next, we present an effective outsourced data integrity auditing technique based on the Merkel sum hash tree (MSHT). Without relying on a third party, our proposed system may simultaneously satisfy the needs of data secrecy and verifiable data update. Simultaneously, the numerical analysis demonstrates that when the number of outsourced subfiles increases, the computing complexity grows logarithmically. Ultimately, a working prototype implementation is created in order to test and emulate our intended method. Chen et al. [16] introduces DisguisedNets, an image-disguising technique that lets users safely send images to the cloud for private, effective GPU-based model training. Training data is transformed using a unique method by DisguisedNets, which combines block-level random permutation, random multidimensional projection (RMT), and AES pixel-level encryption (AES). Without making any changes, users can train models with hidden images using the GPU resources and DNN training techniques that are currently available. We have examined and assessed the techniques using a multi-level threat model and contrasted them with another approach that is comparable, called Instant Hide. A novel steganography method that maintains data integrity and anonymity was presented by Hambouz et al. [17]. By covertly inserting the data pieces into the Steg image, data secrecy is accomplished. The SHA 256 hashing algorithm is used to hash the encoding and decoding variables in order to achieve integrity [18]. Using a dataset of various image sizes, the suggested model achieved high PSNR values, with an average PSNR of 82.933% [19].

Wen et al. [20] in this paper, a matrix-based compressive technique by combining DWT and OMP with chaos. First, the chaotic measurement matrix is improved using the orthogonal optimization method. By using the Kronecker product in conjunction with the Part Hadamard matrix, a measuring matrix with strong orthogonal features is created. Second, DWT only partially captures the original image. In the meanwhile, the association between its neighboring pixels is disrupted using Arnold scrambling [21]. After that, the image is measured and compressed using compressive sensing principles to create an intermediate image that can be encrypted. Qin et al. [22] proposesa encrypted image retrieval the enhanced Harris method. The feature vectors for each image are then produced by applying the BOW (Bag of Words) model and the SURF (Speeded-Up Robust Features) algorithm. The searchable index for the feature vectors is then created using the LSH (Local Sensitive Hash) algorithm. Images are secured using the chaotic encryption system, which also provides index security. Lastly, the cloud server runs a secure similarity search. The proposed retrieval system enhances image retrieval accuracy and reduces time consumption when compared to the current encrypted retrieval schemes, according to experimental data.

In order to create a key for the encryption process, the image is encrypted by Jamil et al. [23]. According to the domain of the feature that was extracted. This is a new path for the research on encryption methods. The application of edges detection initiates the encryption process. The diffusions on the bits are used to produce a key that is utilized to encrypt the edge image after the bits of the edge image have been divided into (3 × 3) windows. To find out if the created key is acknowledged as true, four randomness tests are run through the NIST randomness tests. In order to recover the original image, this decryption process is reversible. The obtained encryption image can be applied to any cyber security domain, including healthcare institutions. Selvaraj et al. [24] looked into the security of medical imaging on the IoT research employing optimization techniques and a novel cryptography model. For patient information and medical images to be securely stored and transported, a unique framework is required [21]. Jia et al. [25] presents feature classification that integrates homomorphic encryption for dividing images in a separate form. We develop a compound encryption technique that makes use of homomorphic computation to counteract the intrinsic complexity of encryption, with the specific goal of reducing computational and storage overheads. Our approach, which is clearly better than traditional ones, offers significant advantages in terms of computational efficiency, lower storage and transmission costs, and strong security and privacy preservation.

The overall highlight of this research includes; a number of researchers have made significant theoretical and practical advances in the application of chaos to image encryption. The model presented a picture encryption that effectively decreased the transmission cost by combining compressive sensing, DNA encoding, and a four-winged hyperchaotic system. This technique avoids the issue of additional key transmission across the channel by using the algorithm known as RSA to encrypt the plaintext key and reveal the associated ciphertext key. Even with limited resources, this technique manages to maintain network system security and availability inside the cloud environment.

3. Proposed work

The proposed model is presented in this section which employs effective extraction of feature and privacy preservation of extracted information in cloud infrastructure where the infrastructures may be of Google cloud and AWS for storing of image information’s. An architecture of the proposed model is shown in **Figure 1**. The major intends of this proposed lies in presenting feature extraction of secret image using optimization model and to employ security preservation scheme on this extracted information with signature verification process before sending the extracted data to user into cloud environment. Thus, the confidentiality of data is enhanced.

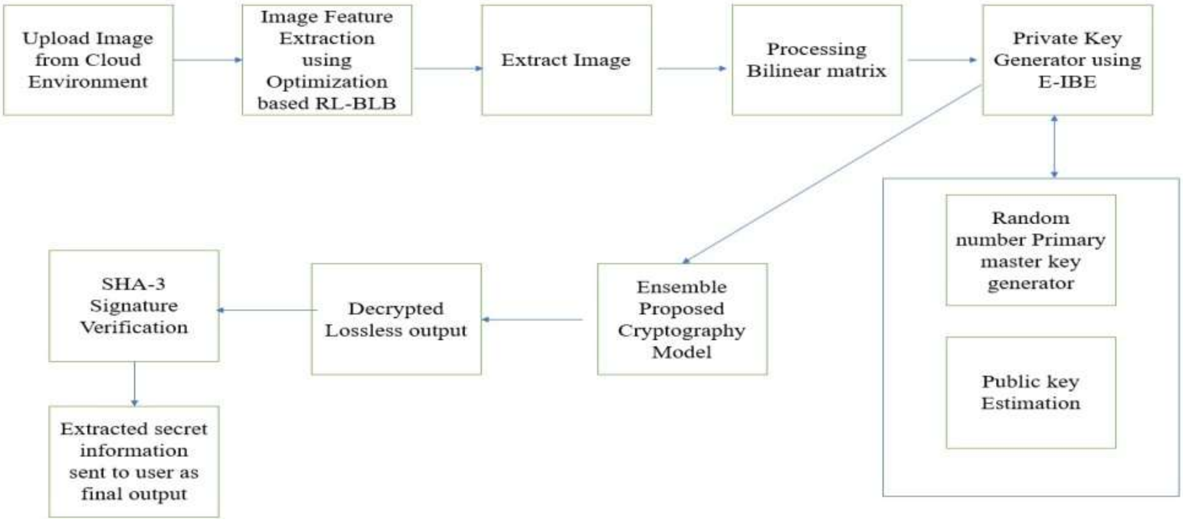

Upload Image from Cloud Environment
Image Feature Extraction using Optimization based RL-BLB
Extract Image
Processing Bilinear matrix
Private Key Generator using E-IBE
Random number Primary master key generator
Public key Estimation
Ensemble Proposed Cryptography Model
Decrypted Lossless output
SHA-3 Signature Verification
Extracted secret information sent to user as final output

Figure 1. Representation of proposed model flow.

3.1. Enriched shark smell optimization based RI-LBP for Image feature extraction

From the considered input dataset, image features are extracted so as to retrieve secret information to the user. The feature extraction of image is carried using Rotational Invariant-Local Binary Pattern (RI-LBP) approach. The feature extraction also employs optimization process so as to select best features by means of attaining best fitness function values [11,12].

The RI-LBP model is attained on rotating every bit pattern circularly to a minimum value, whereas, the traditional LBP is based on uniform patterns. The instance for RI-LBP is provided by: for example, sequences of bit 11000011, 11100001, and 01111000 came from varied rotations of similar local patterns, & they will correspond to normal sequence 00001111 [13]. It means that entire patterns from ingle bin rows are thus replaced using single label. In this, Fast Fourier Transform mechanism is employed for computing the global features from the uniform histogram of LBP in spite of computing the invariants of every pixel in an independent manner [14]. It makes RI-LBP a feature subset of LBP-Histogram features. Depending on the property, that states rotation induces shift of polar representations of neighborhood (P, R), LBP-HF offers class features which are invariant to input image rotation termed features calculated among the rows of input histogram that are invariant to the cyclic shifts. For LBP histogram, FFT is applied by:

$$H(n,u) = \sum_{r=0}^{P-1} h_I(U_P(n,r))e^{-i2\pi ur/P} \tag{1}$$

here, $h_I(U_P(n,r))$ denotes specified uniform histogram of LBP pattern. By this, the features are extracted which is selected by means of employing optimization model for attaining best subset features using Enriched Shark Smell Optimization algorithm.

Enriched shark smell optimization approach

The best fitness function value is attained by means of employing this algorithm so as to select best optimum set of features. Sharks are having foraging behavior due to its nature of best hunting process which undergoes forward and rotations that could be efficient for identifying the prey extremely. The algorithm of optimization to simulate the foraging of shark is effective highly. For any such provided location, sharks move at the speed of particles which have extra penetrating odor, thus NP initial velocity vectors is expressed by:

$$V_1^1, V_2^1, \dots, V_{NP}^1 \tag{2}$$

A shark has the inertia once it swims, such that formulation of velocity for every measurement is given by:

$$V_{i,j}^k = \eta_k . R_1 . \frac{\partial(OF)}{\partial x_j} |_{x_{i,j}^k} + \alpha_k . R_2 . v_{i,j}^{k-1} \tag{3}$$

In this, $j = (1, 2, \dots, ND), i = (1, 2, \dots, NP),$ k signifies phases number, and OF denotes objective function. The sharks might not reach its speed as indicated by gradient function of every stage, such that set $\eta_k \in [0,1]$. At which, R_1 *and* R_2 specifies random number [0,1] termed gradient item. α_k is likewise the random number among [0, 1] denoted by inertia coefficient or the change in momentum rate. The shark's speed is bounded, with their limit formula specified by:

$$|V_{i,j}^k| = min\left[\left|\eta_k . R_1 . \frac{\partial(OF)}{\partial x_j} |_{x_{i,j}^k} + \alpha_k . R_2 . v_{i,j}^{k-1}\right|, |\beta_k . V_{i,j}^k|\right] \tag{4}$$

Here, $j = (1, 2, \dots, ND),\ i = (1, 2, \dots, NP), k = (1, 2, \dots, k_{max}), and\ \beta_k\ is\ the\ milit\ factor\ of\ speedat\ phase\ k.$ The $V_{i,j}^k$ magnitude is attained from above equation. The sharks are having newer position as Y_i^{k+1} due to forward movement, and this Y_i^{k+1} will be identified by existing position and speed and is denoted as:

$$Y_i^{k+1} = X_i^k + V_i^k . \Delta t_k \tag{5}$$

In this, $i = (1, 2, \dots, NP), k = (1, 2, \dots, k_{max}), \Delta t_k$ is the time interval of phase k. Each velocity component of V_i^k velocity is obtained from above expression. Besides move forward, usually sharksrevolve alongside its pathway for looking into the strong odor substances and thus enhance its way of drive which will be moving in actual path. A shark that are rotating, thus travels along closed intervals which is not necessarily circle. As seen from optimization view, sharks thus implement a local search in every phase so as to identify best candidate solutions. For this position, the search formula is denoted by:

$$Z_i^{k+1,m} = Y_i^{k+1} + R_3 . Y_i^{k+1} \tag{6}$$

In this, m = (1, 2, …, M), and R_3 symbolizes random number among [−1,1], M denotes number of points at every stage of search location. In case, the shark identifies strong point of scent in rotational movement, this moves towards points thereby continues path of search. A search formula for location is denoted by:

$$X_i^{k+1} = \text{arg max}\{OF(Y_i^{k+1}),\ OF(Z_i^{k+1,1}), \dots, OF(Z_i^{k+1,M})\} \tag{7}$$

From above expression, Y_i^{k+1} is attained from linear movement $\&Z_i^{k+1,1}$ from rotational movement. The sharks might select the candidate solution X_i^{k+1} which are having high value of evaluation index as the next location of shark.

3.2. Initialization of parameter and private key generator using E-IBE

The bilinear matrix is carried for parameter initialization followed by generation of private key using E-IBE. A flow diagram of the proposed model is shown in **Figure 2** description of this is shown in here.

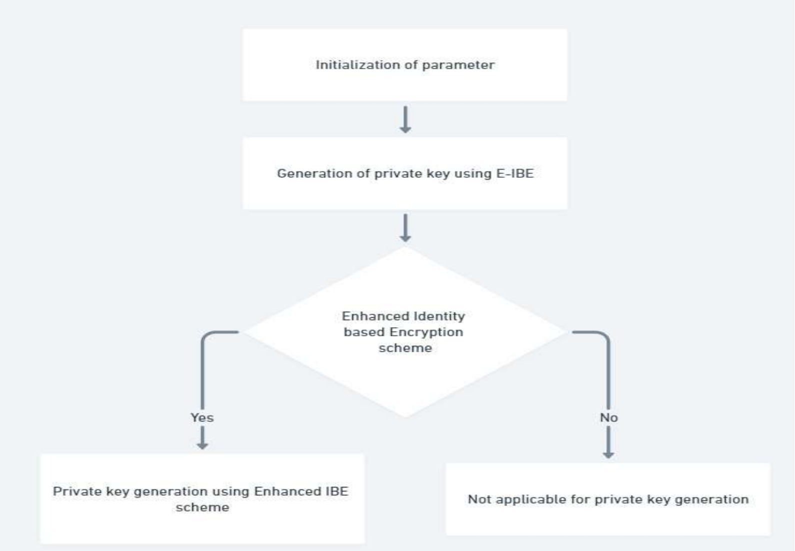

Initialization of parameter
Generation of private key using E-IBE
Enhanced Identity based Encryption scheme
Yes
No
Private key generation using Enhanced IBE scheme
Not applicable for private key generation

Figure 2. Flow diagram for private key generator.

3.2.1. Bilinear matrix for parameter initialization

At initialization phase, client thus generates common parameters to unify entire system modules. Depending on the initialization of parameter and prime numbers, cloud server offers bilinear matrix model. The mapping of bilinear mapping is regarded as a complex task which is employed on the cryptographic protocols along with the key generation process based on Enhanced IBE. Assume, C_1 & C_2 be the two cyclic additive groups that have generators G_a & G_b correspondingly. Let n be the large prime number at direction C_1 & C_2. Let C_T regarded as cyclic multiplicative group having n arrangements. The mapping of m is denoted as bilinear pairing: which has $C_1 \times C_2 \rightarrow C_T$ which satisfies following properties:

- Bilinear: $m\,(aP, bR) = m\,(P, R)^{a \times b}$ for any such $P \in C_1 \& R \in C_2 \& a, b \in Z_n^*$.
- Non-degenerate: which is at any $P \in C_1 \& R \in C_2$ so that $m\,(P, R) \neq 1$.
- Computable: computing $m\,(P, R)$ for entire $P \in C_1 \& R \in C_2$.

A bilinear set of the cloud server is signified by:

$$Parameter = (C_1, C_2, C_T, G_a, G_b, n, m, P, R) \leftarrow G(1_\lambda) \quad (8)$$

In the above equation, security parameter is denoted by λ & bilinear matrix properties are thus satisfied by other parameters.

Followed by bilinear matrix parameter initialization, the key generation process takes place using Enhanced Identity based Encryption scheme (E-IBE).

3.2.2. Enhanced identity based encryption scheme

For the purpose of private key generation, Enhanced IBE scheme is employed. This IBE is a quicker version at which the users were allowed for accessing the data with the use of their identity by means of authentication. This model is implemented initially at proxy servers so as to revoke the unauthorized users. In the proxy server, authorized users' identity is thus kept, & wherever the unauthorized user attempts to access service in server, they will attain a revoked since there is no such matching of key for that desired identity. Thus, every user should register their identity to access service.

Let Alice and Bob be the two users using cloud resources and private key generator that authenticates to access cloud databases. This model depicts in what way the Alice and Bob access data of each one through employing IBE as authentication model, authorization, and a security tool. The unauthorized user is not capable of getting the identity of authorized user since PKG maintains the user's identity in the form of Lagrange polynomial that is hard computationally for an outside attacker to get crack and attain original identity. In case, Bob sends their identity to Alice in middle of communication, the attacker might not get that identity since they are shared with the use of secure socket connection (SSL). As the hash-based key generation models are expensive computationally, pairing dependent key generation model is employed in this work. The E-IBE model is described as shown below:

Assume G be the group of the prime order p. The G forms computable bilinear map proficiently into $G1$. The representation of bilinear map $G1$ is expressed by $e: G \times G_1 \rightarrow G_2$, & g denotes group G generator. A security parameter is employed for identifying group size, & thereby identities are signified by four strings having length $n.4$.

$$\mathrm{ID} = (\mathrm{id}_1, \mathrm{id}_2, \mathrm{id}_3, \dots, \mathrm{id}_n) \tag{9}$$

A collision free function of hash could be employed for generating fixed length bit strings n from arbitrary length ID of bit strings. The subsequent stages are included in the suggested algorithm.

Step 1: Setup phase:

Initially, system parameters are generated. The secret is thus chosen randomly from Z_p. Select random generator g from G so that $g \in G$, thereby fixing values of $g1 = g^{\alpha}$& thereby selects u random numbers which is indicated as $U = \{u_i\}$. At last, g, g_1, g_2, u'& U will be issued to be public parameters &g_2^{α} be master key.

Step 2: Generation phase:

Assume v be n bit string identity for the user, v's ith bit is signified as v_i, at which $V \subseteq \{1, \dots, n\}$ is a set of entire i at which $v_i = 1$. V will be segregated as two different that is $V = \{v_1, v_2, \dots, v_m\}$&$\{v_{r1}, v_{r2}, \dots, v_{rm}\}$ so that $m + r_m = n$, here, v_{ri} signifies random values that is included for offering security for proposed scheme. The identity v will be produced on selecting random value after which a private key corresponds to identity as given below in Equation (10).

$$d_v = \left(g_2^{\alpha} \left(u' \prod_{i \in V} v_i \right)^r, g^r \right) \tag{10}$$

$U = \{u_1, u_2, \dots u_n\}$ and $V = \{v_1, v_2, \dots, v_m\}$ so that $m < n$. In this time, exploit Lagrange coefficient model for generating the function of polynomials for performing polynomial interpolation. This polynomial interpolation aids in hiding some values of v that could be recovered successfully from traditional data points. The proposed model's polynomial equation is given by:

$$P(x) = \frac{(x-x_1)(x-x_2)\dots.(x-x_n)}{(x_0-x_1)(x_0-x_2)\dots.(x_0-x_n)} y_0 + \frac{(x-x_0)(x-x_1)\dots.(x-x_{n-1})}{(x_1-x_0)(x_1-x_2)\dots.(x_1-x_n)} y_1 \dots. \frac{(x-x_1)(x-x_2)\dots.(x-x_n)}{(x_n-x_0)(x_n-x_1)\dots.(x_n-x_{n-1})} y_n \tag{11}$$

The Lagrange coefficient is expressed by:

$$\Delta_{i,v}(x) = \sum_{i=0,k\in V}^{n} \left(\prod_{0<i<n, j\neq i} \frac{x-x_j}{x_i-x_j} \right) y_k \tag{12}$$

here, $x = u_i \& \, y = v_k$. A random set u_i will once be generated for every user identity &LaGrange coefficient is generated for every identity with the use of similar values of u_i. The authority might employ m-terms of the identity values because of this attacker might never know uniqueindividuality of that officialuser. Therefore, this might be harder for attaining or guessing key generated for that specified ID. In the case, if entire values of user ID and U will be similar, error produced by *P*(*x*) will be zero, i.e., the attacker might not capable of guessing anything from that key. In this superior case, note that generated error might be 0 & among 2 successive nodes, the maximum errors might be recognized.

Step 3: Encryption phase:

Consider 'c' as a random value that is selected from Z_p & message $M(M \in G_1)$. In some identity *v*, the process of encryption will be carried by means of following equation:

$$C = \left(e(g_1, g_2)M, g^c, \left(u' \prod_{i\in V} v_i \right)^c \right) \tag{13}$$

Step 4: Decryption phase:

Assume $C = (C_1, C_2, C_3)$ as a valid text of cipher for the *M* message under the identity of user *v*. After that, the *C* cipher text might be decrypted by means of $d_v = (d_1, d_2)$ which is expressed by following equations:

$$(e(g_1, g_2)^c M) \frac{e(g^r, (u' \prod_{i=V} v_i)^c)}{e(g_2^\alpha (u' \prod_{i\in V} v_i)^r, g^r)} \tag{14}$$

$$(e(g_1, g_2)^c M) \frac{e(g, (u' \prod_{i=V} v_i)^{rc})}{e(g_1, g_2)^c e((u' \prod_{i=V} v_i)^{rc}, g)} \tag{15}$$

$$(e(g_1, g_2)^c M) \frac{e(g, (u' \prod_{i=V} v_i)^{rc})}{e(g_1, g_2)^c e(g, (u' \prod_{i=V} v_i)^{rc})} \tag{16}$$

$$\mathrm{C} = M. \tag{17}$$

Hence, by this, the private key is generated and is followed by cryptographic scheme which is shown in subsequent section.

3.3. Ensemble improved homomorphic pailler and quantized elgammal ECC for cryptography

An Ensemble improved Homomorphic Pailler& Quantized Elgammal ECC cryptosystem is employed to secure the data.

3.3.1. Pailler cryptosystem

This pailler based encryption is a semantic secured and probabilistic encryption which is also a homomorphic one. This is not as much as strong like FHE which has both multiplicative & additive possessions similarly; however, this is much more practical and sophisticated. This multiplicative and additive property indicates that it is capable of computing encrypted sum or the product of 2 numbers over computing ciphertexts of the respective numbers with that of public keys. This additive nature aids data owner to preserve secret key confidentially thereby protecting data of user quality through secured multiplication. This model includes 3 phases like key generation together with encryption & decryption. In the key generation process, 2 large prime numbers a and b are selected randomly. The calculation of these terms n and $\lambda(n)$ are computed by $n = ab$, after which:

$$\lambda(n) = \mathrm{lcm}(a-1, b-1) \tag{18}$$

After which, generator element t & μ are chosen by:

$$\mu = (L(t^{\lambda} mod\, n^2))^{-1}\, mod\, n \tag{19}$$

In this, $L(p)$ is signified by $L(p) = (p-1)/p$. Therefore, public key is signified by (n, t), and private key as (λ, μ). Once the key is generated then g is encrypted using:

$$CT = t^g, k^n\, mod\, n^2 \tag{20}$$

In this, k is regarded as random number. After that, ciphertext is being decrypted by means of following equation:

$$g = (L(CT^{\lambda} mod\, n^2)/L\,(t^{\lambda} mod\, n^2))mod\, n \tag{21}$$

This model is hybridized with Quantized Elgammal ECC model so as to attain enhanced security performance [26].

3.3.2. Quantized elgammal ECC

A Quantized Elliptic curve will be described as a point that satisfies Weierstrass equation in plane projection. Assume E_p as elliptic curve notation and is expressed by:

$$y^2 = x^3 + ax + b(mod\, p) \tag{22}$$

In this, 'a' & 'b' signifies 2 constants which satisfies $4a^3 + 27b^2 \neq 0$, and p signifies the prime. Specifically, the coordinates of EC must follows the Abelian additive property.

Definition 1*:* EC Addition: Assume $P, Q, R, and\ O$ be the 4 points at EC (Elliptic curve) E_p (O denotes the infinite points) [27]:

(a) $O + P = P + O = P$;

(b) $-O = O$;

(c) In case $P(x, y) \neq 0$, after that $-P =(x, -y)$;

(d) In case $Q = -P$, after that $P + Q = 0$;

(e) In case $P \neq Q, Q \neq O$, $Q \neq -P$, R signifies other straight lines intersection PQ (if $P \neq Q$)orelse E_p in point of intersection P if $P = Q$) having other EC point E_p, after that, $P + Q =$ âĹ′R [24].

From **Figure 3**, $P(x_1, y_1)$ & $Q(x_2, y_2)$ will be regarded as elliptic curve randomly, and in another point R of EC, straight line is constructed. Then, the y axis parallel axis will be crossed over R to R', & prompt $P(x_1, y_1) + Q(x_2, y_2) = R' = -R = (x_3, -y_3)$. Therefore, result of additional point $R'(x_3, y_3)$ will be denoted by [28]:

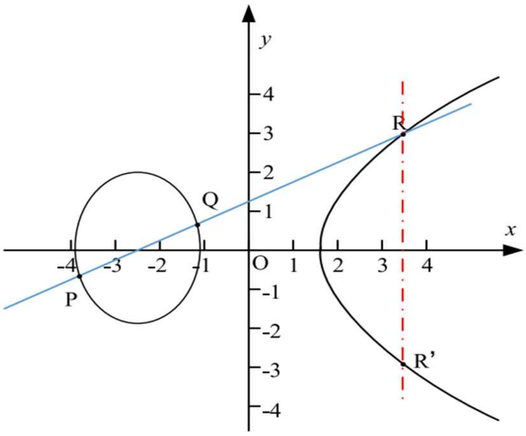


Figure 3. Theory of EC encryption.

$$\begin{cases} x_3 = \tau^2 - x_1 - x_2 \\ y_3 = \tau(x_1 - x_3) - y_1 \end{cases} \tag{23}$$

In this, τ signifies slope and is denoted by:

$$\tau = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if\ P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & if\ P = Q \end{cases} \tag{24}$$

As of the analysis shown above, it was obvious that result of point addition is entirely on EC. However, addition integration law on EC and discrete logarithm function, the EC based cryptography should be established. The EC Discrete Logarithm Problem (ECDLP) must be established. This is the asymmetric cryptosystem that may create cryptosystem security depending on ECC.

Definition 2*:* Let p be the prime & elliptic curve is denoted by E_p. Intended for P and Q be 2 points on the EC, which must satisfy the condition $Q = kP$. It is obvious that it must be easier for computing Q from k & P. Though, this might be intricate for computing k from P and Q.

Due to irreversible ECDLPsolution, cryptosystem ElGammalwill be presented & is thus defined by Quantized ElGammal cryptosystem that offers faster computation with smaller length of key. Though, security is offered by Quantized ElGammal

Elliptic cryptosystem will be enhanced than others. The process of encryption and decryption is provided by [29]:

Stage 1: Generation of key at receiver side

(a) Elliptic curve Equation $E_p: y^2 = x^3 + ax + b, p$ prime & L basic point were selected.

(b) A private key d will thus be set by the receiver & Q is computed by means of $Q = \mathrm{dL}$.

(c) E_p, p, L, Qkeys remains visible

Stage 2: process of transmitter's encryption:

(a) A plain text is signified by U, & it is converted as points on EC filed as U'.

(b) A $private\ key\ k$ will be set by transmitter once $C_1 = kL \& C_2 = U' \otimes kQ$, at which $' \otimes '$ signifies addition operation on EC.

(c) An encrypted data $C_1 \& C_2$will thus be transmitted to receiver.

Stage 3: process of decryption by transmitter

(a) As per private key d of the receiver, U'will be specified as:

$$U' = C_2 \oslash dC_1 = (U' \otimes kQ) \oslash d(kL) = U' \otimes (k.dL\ \oslash d.kL) = U' \tag{25}$$

In this, " $\oslash$ " signifies to the inverse addition operation on EC.

(b) From plaintext to $U'\ to\ U$ restoration.

Since the existing models such as RSA needs huge size of keys, computation time might be higher and likewise the process also expensive. It should be avoided using this proposed Ensemble model thereby offering security with smaller key size and less time. Since the additive homomorphic encryption is followed, the suggested model executes simple addition over integers for the purpose of encryption and decryption process [30].

3.4. SHA3 based signature verification

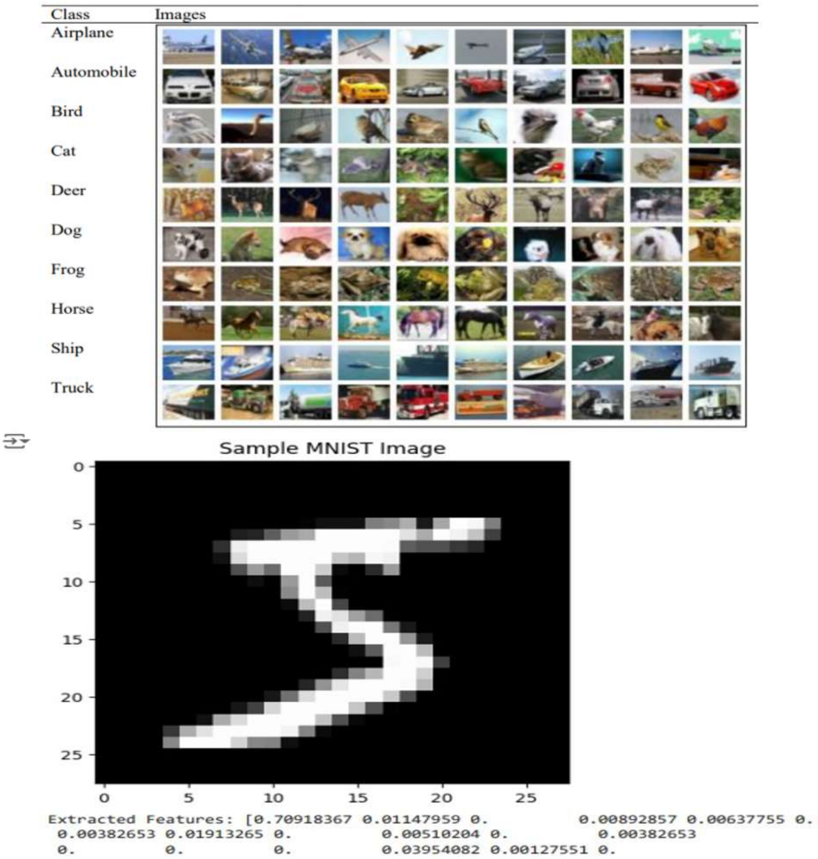
At last, the verification of signature is accomplished on the decrypted outcome using SHA3 based hashing function so as to access authenticated users. Generally, hash function exploits variable length data blocks as an input and provides fixed hash values size. this hash function thereby checks integrity of data and alters in any data bits might offer other hash value. For any such data selected *D*, it is complicated to extract data *M* such that *H*(*D*) = *M*. The existing hashing technique limitation is overcome on employing this model. Therefore, this proposed hash function is a type of computing signatures of several magnitudes such as 224, 256, 384 & 512 bits. There exist two stages like squeezing and absorbing stage. In absorption phase, original text is thus exposed to the transformation and in squeezing phase, hash value output is condensed from initial bit & after that permutations will be carried if bit needed is not accomplished at output. Therefore, resulting value output of permutations are computed. An efficient security constraint for generic attacks are major intention of SHA3. The function of compression is flexible and simpler. By this, one-way password for SHA3 is created for member authentication and verification of signature is carried by means of hash function [31].

4. Performance analysis

The performance evaluation of feature extraction image categorization for secret data sharing is tested and the evaluations made are projected here. The performance is tested on CIFAR-10 and MNIST based image dataset at which these input images are shared with secret data. The proposed model extracts the features of these images thus categorizes based on their features to extract secret message.

4.1. Performance evaluation with considered database with feature extraction categorization model

A dataset CIFAR-10 and MNIST [26] comprises of several images employed for training ML approaches & computer vision. Thus, presented database will be utilized progressively intended for the ML approach-based retrieval process. It has about 60,000 images, entire of which having size 32 × 32 and in the format of PNG with ten different classes as shown in below **Figure 4**. For instance, a vehicle, an Aeroplan, birds, cat, deer, dog, horse, frog, truck, and ship are the classes. Total of about 5000 training pictures with 10,000 testing images are considered from dataset CIFAR − 10 and MNIST sample images along with first set being exploited for training and next set employed for testing for estimating suggested model. There exist 1000 photos precisely from every class of testing batch which were picked arbitrarily. The arranged 5000 images randomly from every class will be covered at every training batch.



```
Extracted Features: [0.70918367 0.01147959 0.         0.00892857 0.00637755 0.
 0.00382653 0.01913265 0.         0.00510204 0.         0.00382653
 0.         0.         0.         0.03954082 0.00127551 0.
```

Figure 4. Input image from CIFAR and MNIST database classes.

Figure 5 is the extraction accuracy outcome and its comparison with existing models. The accuracy of feature extraction model employed is estimated and their outcomes are related with other extraction models considered. From analysis, it is obvious that the proposed model (RI-LBP) with optimization model enhances the accuracy of feature extraction process [32].

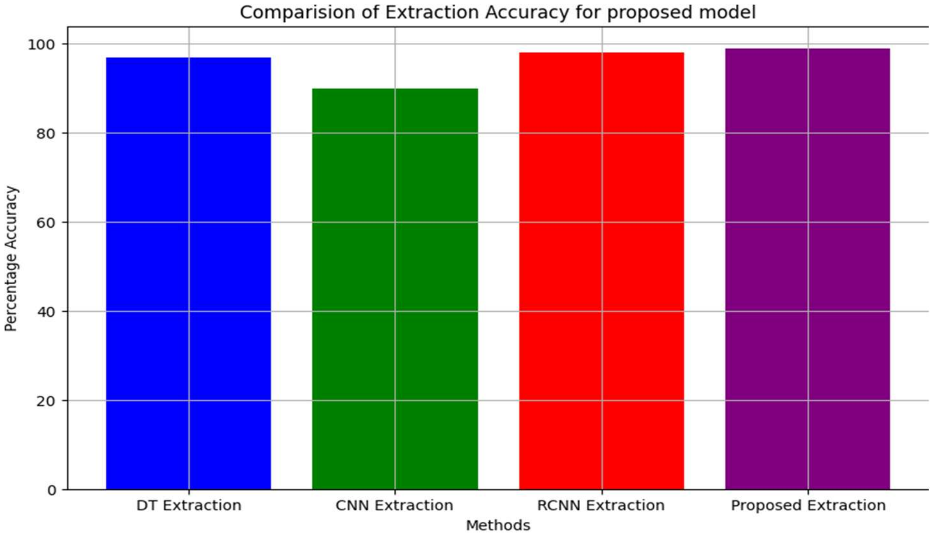
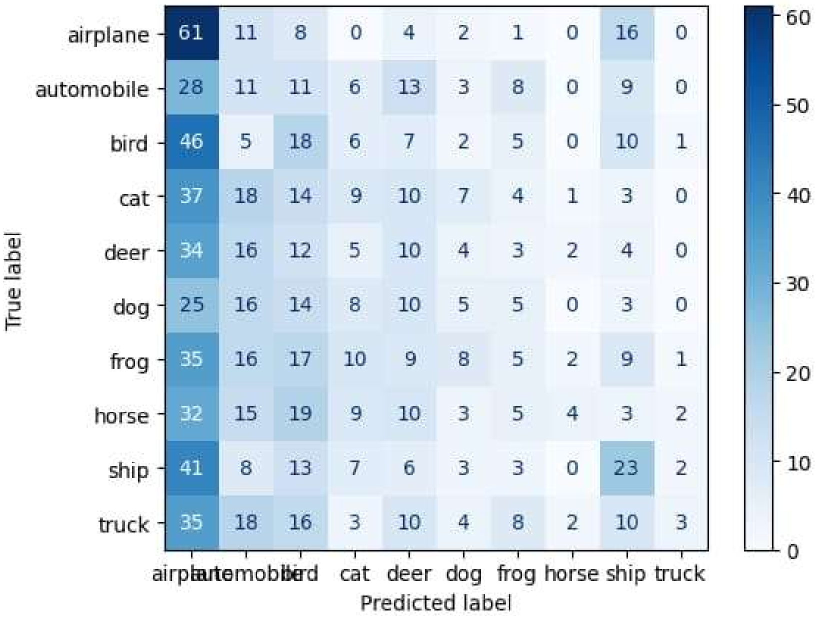


Figure 5. Extraction accuracy.

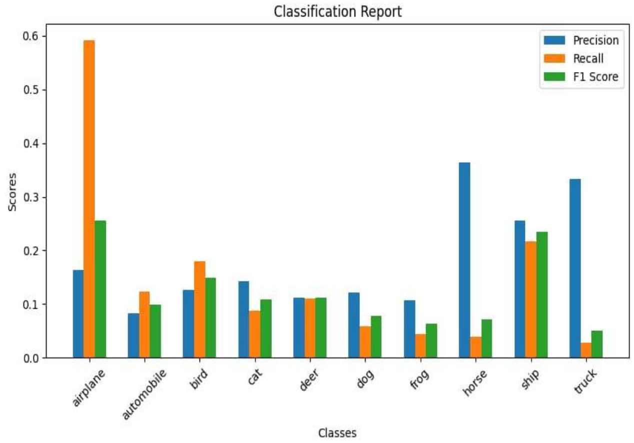
The extracted categorization outcome is compared with actual outcome and the confusion matrix for predicted and true labels are projected and is shown in **Figure 6**.



	airplane	automobile	bird	cat	deer	dog	frog	horse	ship	truck
airplane	61	11	8	0	4	2	1	0	16	0
automobile	28	11	11	6	13	3	8	0	9	0
bird	46	5	18	6	7	2	5	0	10	1
cat	37	18	14	9	10	7	4	1	3	0
deer	34	16	12	5	10	4	3	2	4	0
dog	25	16	14	8	10	5	5	0	3	0
frog	35	16	17	10	9	8	5	2	9	1
horse	32	15	19	9	10	3	5	4	3	2
ship	41	8	13	7	6	3	3	0	23	2
truck	35	18	16	3	10	4	8	2	10	3

Figure 6. Confusion matrix of true labels and predicted labels.

Figure 7a is the categorization report attained for each class with respect to precision, recall, and F1-score for varied classes. For entire classes, the calculations of entire metrics like precision, recall, and F1-score are defined in **Figure 7b** [21].



(a)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

$$F1\text{-}score = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

(b)

Figure 7. (a) Categorization report of each class w.r.t precision, recall, F1-score, **(b)** Performance metrics calculation.

The RoC curve is plotted in terms of false positive rate and true positive rate of extraction process. The categorization of extracted image is predicted for their false and true predictions from which the RoC curve plot is carried and is shown in **Figure 8**.

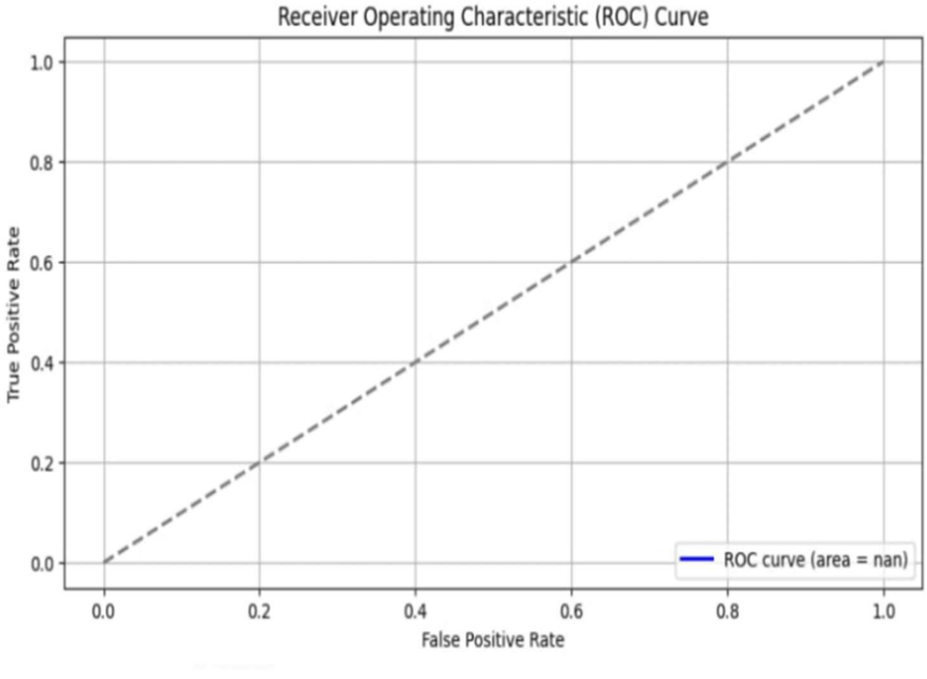


Figure 8. ROC curve.

The precision-recall curve is plotted in terms of precision values and recall values attained from proposed extraction process. The categorization of extracted image is predicted for its precision and recall values from which the precision-recall curve is plotted and is shown in **Figure 9** [33].

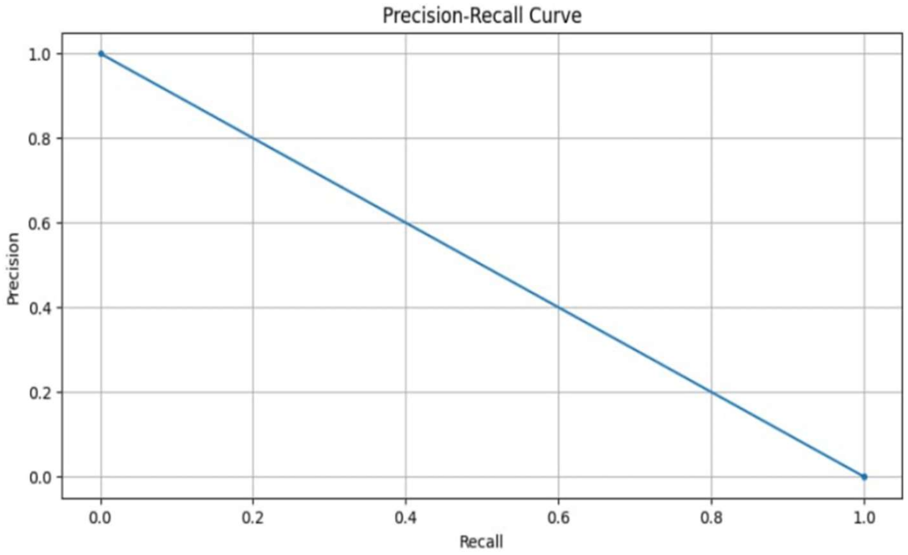


Figure 9. Precision-recall curve.

4.2. Comparative estimation of proposed cryptography and key generation schemes

Once the feature extraction and categorization of extracted features are made, the cryptographic approach is employed to make the data transmission secure. The performance of this security model employed is estimated and is compared with existing models to prove the enhancement of proposed model over others.

Figure 10 represents the comparative analysis of runtime of whole process. From this, it was evident that proposed method takes less time on comparing other existing techniques like BCAS and tuCP-ABE scheme. As the attributes increases, the runtime of whole process of the existing technique is longer than the proposed method which reveals the effectiveness of proposed scheme [27]. **Figure 11** illustrates the comparative analysis of storage space of the whole process.

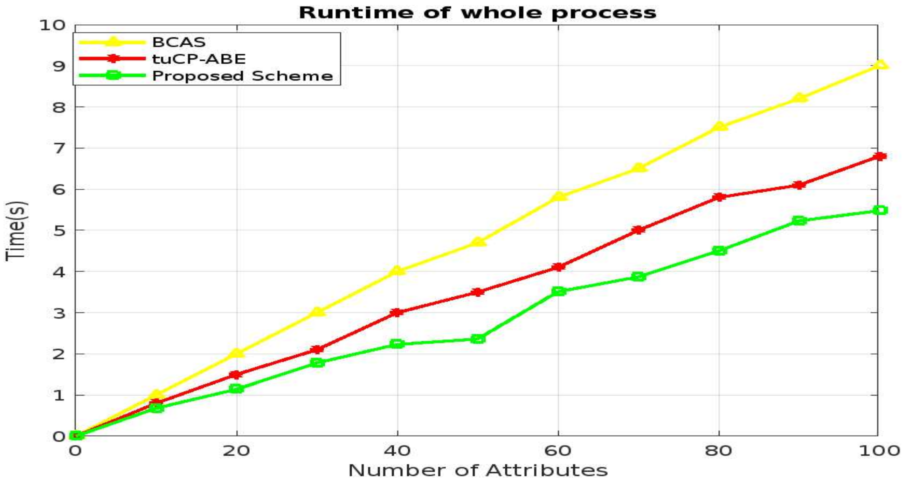


Figure 10. comparative analysis of runtime of whole process.

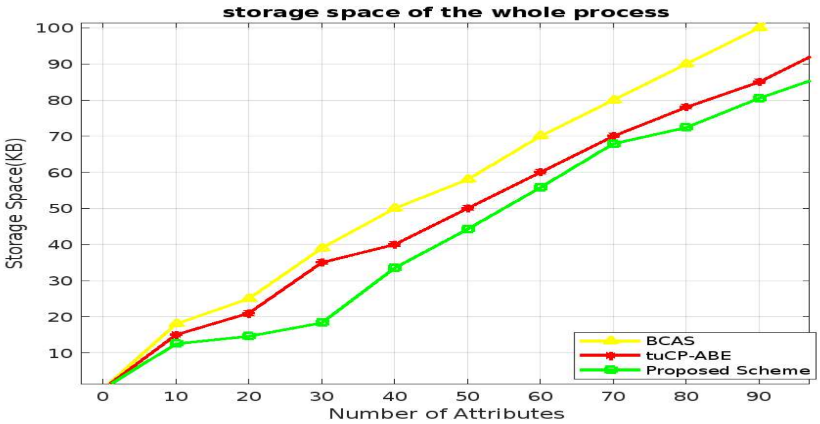


Figure 11. comparative analysis of storage space of whole process.

Figure 12 represents the comparative analysis of storage space of whole process. From this, it was evident that proposed method takes less space on comparing other existing techniques like BCAS and tuCP-ABE scheme. As the attributes increases, the runtime of whole process of the existing technique is longer than the proposed method which reveals the effectiveness of proposed scheme.

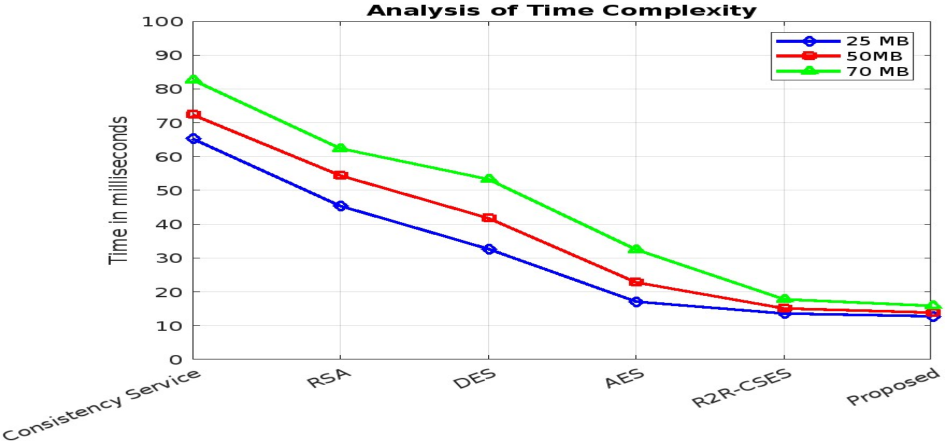


Figure 12. comparative analysis of time complexity.

A time complexity of the suggested method is estimated and outcomes attained are compared with existing methods and is illustrated **Figure 12** and the proposed model time complexity is low compared to other existing model where proposed model time complexity is $O(n)$ and RSA, Variant paillier, Elgamal as $O(n^2)$ where consistency services achieve the worst case of $O(2^n)$. The time complexity is expressed as shown:

$$T_s = \frac{\text{Total number of blocks per bits} \times \text{two phase encryption}}{\text{Time taken } (s)} \tag{26}$$

Table 1 shows the proposed cryptography system execution time employed. The execution time is estimated for both encryption process and decryption process. The results are compared with other existing models [28], Medileh SA, Laouid M, Hammoudeh M, et al. [34] to prove the effectiveness of suggested scheme over other models compared. The analysis attained shows that the execution time of suggested model will be lower than others making system effective. An attained outcome clearly shows that the encryption & decryption speed of suggested system outpaces the existing methods time. Thus, the proposed model is said to have higher speed with enhanced security.

Table 1. comparative analysis of execution efficiency.

Methods	**Encryption Time (ms)**	**Decryption Time (ms)**
Consistency service	68.1	82.4
RSA [28]	55.4	64.4
Variant-Paillier [29]	11.91	17.67
ElGamal [30]	47	15
DGHV [31]	50	10
PRBS-HE [32]	255	493
SGD-HE [33]	899	785
LF-HE [34]	0.07	11.95
P-HE [35]	0.036	0.041
Proposed	0.029	0.038

5. Conclusion

The extraction of image features and transmission of extracted secret information transmission securely in cloud environment was carried in the proposed model. Primarily, input images were retrieved & parameter initialization is carried using bilinear matrix. The Optimal feature extraction is carried using RI-LBP along with Enriched Shark smell optimization process so as to extract secret information's feature. then, the private key generation takes place using E-IBE followed by cryptographic process using Ensemble Improved Homomorphic Pailler & Quantized ElGammal ECC approach. The attained decrypted outcome was then verified digitally by means of SHA3 verification model. The data retrieved is provided to the user after validation securely. The simulation results are then observed on CIFAR-10 database by analyzing proposed scheme performance & comparisons were made with traditional schemes to validate the enhancement of proposed model over other schemes. The performance is carried for various metrics like extraction accuracy, precision, F1-score, recall, RoC curve, precision-recall curve, runtime & storage space of entire system, and execution time. The outcome shows that the proposed model shows improvement over other existing models compared. The future work includes adding more variety of dataset for the image extraction to increase the efficiency of the proposed approach. Furthermore, there aren't many solutions that can effectively accomplish dynamic data updating and data integrity checking at the same time without relying on a third party. Consequently, this research primary goal is to create a novel plan that would address all of the above-mentioned issues at once. In addition to guaranteeing the image's security, the above-mentioned multiple encrypted image retrieval systems might also retrieve comparable images and increase the size of images in future testing environments. However, in future to increase retrieval efficiency, selecting a sensible index construction strategy of images is therefore essential.

Author contributions: Conceptualization, SK and GJE; methodology, SK; software, SK; validation, SK and GJE; formal analysis, GJE; investigation, SK; resources, GJE; data curation, GJE; writing—original draft preparation, SK; writing—review and editing, SK; visualization, SK; supervision, GJE; project administration, SK; funding acquisition, GJE. All authors have read and agreed to the published version of the manuscript.

Funding: None.

Ethical approval: Not applicable.

Informed consent statement: Not applicable.

Acknowledgments: The authors would like to express their heartfelt gratitude to the supervisor for his guidance and unwavering support during this research.

Conflict of interest: The authors declare no conflict of interest.

References

1. Deepa V. Dynamic key generation for securing digital images with chaotic encryption. educational administration: Theory and Practice. 2024; 30(6): 2949–2953. doi: 10.53555/kuey.v30i6.5933
2. Goplakrishnan S, Hussain MZ, Mohd Ashraf G. Senthilkumar, Mantripragada Yaswanth Bhanu Murthy, Sensitive product feature integrity and confidentiality using blockchain-based internet of things (IoT) architecture, Measurement: Sensors. 2023; 27(2023): 100798. doi: 10.1016/j.measen.2023.100798
3. Hua Z, Liu X, Zheng Y, et al. Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing. IEEE Trans. Circuits Syst. Video Technol. IEEE; 2023. doi: 10.1109/TCSVT.2023.3298803
4. Li X, Jiang Y, Chen M, et al. Research on iris image encryption based on deep learning. EURASIP J. Image Video Process. 2018; 2018: 126. doi: 10.1186/s13640-018-0358-7
5. Man Z, Li J, Di X, et al. Double image encryption algorithm based on neural network and chaos. Chaos Solitons Fractals. 2021; 152: 111318. doi: /10.1016/j.chaos.2021.111318
6. Xu Z, Ahmad, Suzana, et al. Image feature extraction algorithm based on visual information. Journal of Intelligent Systems. 2023; 32, 1(2023): 20230111. doi: 10.1515/jisys-2023-0111
7. Kumar S. Aanjan, Monoj Kumar Muchahari S, et al. Application of hybrid capsule network model for malaria parasite detection on microscopic blood smear images. Multimedia Tools and Applications. 2024; 1–27(2024). doi: 10.1007/s11042-024-19062-6
8. Wen H, Lin Y. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Systems with Applications. 2024; 237: 121514. doi: 10.1016/j.eswa.2023.121514
9. Wen H, Lin Y, Yang L, et al. Cryptanalysis of an image encryption scheme using variant Hill cipher and chaos. Xpert Systems with Applications. 2024. doi: 10.1016/j.eswa.2024.123748
10. Chai X, Fu J, Gan Z, et al. Exploiting Semi-Tensor Product Compressed Sensing and Hybrid Cloud for Secure Medical Image Transmission. IEEE Internet of Things Journal. 2023; 10(8): 7380–7392. doi: 10.1109/jiot.2022.3228781
11. Ye G, Liu M, Yap WS, et al. Reversible image hiding algorithm based on compressive sensing and deep learning. Nonlinear Dynamics. 2023; 111: 13535–13560.
12. Aanjankumar S, Poonkuntran, S. Peer-2-Peer Botnet manage SDT security algorithm. In: 2016 IEEE international conference on computational intelligence and computing research (ICCIC). IEEE; 2016. pp. 1–5.
13. Chen Z, Ye G. An asymmetric image encryption scheme based on hash sha-3, rsa and compressive sensing. Optik. 2022; 267: 169676. doi: 10.1016/j.ijleo.2022.169676
14. Liang J. A secure and effective image encryption scheme by combining parallel compressed sensing with secret sharing scheme. International Journal of Information Security. 2023; 75: 103487. doi: 10.1016/j.jisa.2023.103487
15. Yang C, Song, Bowen, et al. Efficient data integrity auditing supporting provable data update for secure cloud storage. Wireless Communications and Mobile Computing. 2022; 1–12. doi: 10.1155/2022/5721917

16. Chen K, Gu Y, Sharma S. DisguisedNets: Secure image outsourcing for confidential model training in clouds. ACM Transactions on Internet Technology. 2023; 23: 3.doi: 10.1145/3609506
17. Hambouz A, Shaheen Y, Manna A, et al. Achieving Data Integrity and Confidentiality Using Image Steganography and Hashing Techniques. In: Proceeding of 2019 2nd International Conference on new Trends in Computing Sciences (ICTCS). 2019; 1-6. doi: 10.1109/ictcs.2019.8923060
18. Goswami, Paromita, Faujdar, et al. Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. Journal of Cloud Computing. 2024; 13. doi: 10.1186/s13677-024-00605-z
19. Li M, Jiang Y, Zhang Y, et al. Medical image analysis using deep learning algorithms. Front. Public Health. 2023.doi: 10.3389/fpubh.2023.1273253
20. Wen H, Yang L, Bai C, et al. Exploiting high-quality reconstruction image encryption strategy by optimized orthogonal compressive sensing. Scientific Reports. 2024; 8805(2024). doi: 10.1038/s41598-024-59277-z
21. Alsafyani M, Alhomayani F, Alsuwat H, et al. Face Image Encryption Based on Feature with Optimization Using Secure Crypto General Adversarial Neural Network and Optical Chaotic Map. Sensors. 2023; 23: 1415. doi: 10.3390/s23031415
22. Qin J, Li H, Xiang X, et al. An encrypted image retrieval method based on Harris corner optimization and LSH in cloud computing. IEEE Access. 2019; 7: 24626-24633. doi: 10.1109/access.2019.2894673
23. Salim J, Abeer, Azeez, et al. An image feature extraction to generate a key for encryption in cyber security medical environments. International Journal of Online and Biomedical Engineering (iJOE). 2023; 19: 93-106.doi: 10.3991/ijoe.v19i01.36901
24. Selvaraj J, Lai WC, Kavin BP, et al. Cryptographic encryption and optimization for internet of things based medical image security. Electronics. 2023; 12: 1636. doi: 10.3390/ electronics12071636
25. Jia H, Cai D, Yang J, et al. Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network. Journal of Cloud Computing. 2023; 12, 175(2023). doi: 10.1186/s13677-023-00537-0
26. Alsaedi EM, Kadhim FA. Retrieving encrypted images using convolution neural network and fully homomorphic encryption. Baghdad science journal. 2023; 20(1): 0206-0206.doi: 10.21123/bsj.2022.6550
27. Kumar S, Aanjan P, Karthikeyan S, et al. Protecting medical images using deep learning fuzzy extractor model. In: Deep Learning for Smart Healthcare. Auerbach Publications; 2024. pp. 183-203.doi: 10.1201/9781003469605
28. Indira N, Rukmanidevi S, Kalpana AV. Light weight proactive padding based crypto security system in distributed cloud environment. International Journal of Computational Intelligence Systems. 2020; 13, 1(2020): 36-43.doi: 10.2991/ijcis.d.200110.001
29. Pang H, Wang B. Privacy-preserving association rule mining using homomorphic encryption in a multikey environment. IEEE Systems Journal. 2020; 15, 2(2020): 3131-3141.doi: 10.1109/JSYST.2020.3001316
30. Aanjankumar S, Poonkuntran S. An efficient soft computing approach for securing information over GAMEOVER Zeus Botnets with modified CPA algorithm. Soft Computing. 2020; 24, 21(2020): 16499-16507.doi: 10.1007/s00500-020-04956-y
31. Coron JS, Mandal A, Naccache D, et al. Fully homomorphic encryption over the integers with shorter public keys. In: Annual Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg; 2011. pp. 487-504.doi: 10.1007/978-3-642-22792-9_28
32. Dasgupta, Smaranika, Pal SK. Design of a polynomial ring based symmetric homomorphic encryption scheme. Perspectives in Science. 2016; 8(2016): 692-695.doi: 10.1016/j.pisc.2016.06.061
33. Boer D, Kramer S. Secure sum outperforms homomorphic encryption in (current) collaborative deep learning. arXiv; 2006.doi: 10.48550/arXiv.2006.02894
34. Medileh SA, Laouid M, Hammoudeh M, et al. A multi-key with partially homomorphic encryption scheme for low-end devices ensuring data integrity. Information. 2023; 14: 263.doi: 10.3390/info14050263