Journal of Information Systems Engineering and Management
2025, 10(5s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Development of Security Aware Content Based Image Retrieval System using Lightweight Trapdoor Verification in Cloud Environment

[1]Pushpanjali Munnalal Chouragade*, [2]Premchand B. Ambhore
[1] Research Scholar
Computer Science & Engineering
Government College of Engineering, Amravati
pushpanjalic3@gmail.com
[2]Assistant Professor
Information Technology
Government College of Engineering, Amravati

ARTICLE INFO

Received: 08 Oct 2024

Revised: 09 Dec 2024

Accepted: 24 Dec 2024

ABSTRACT

Demand for personal privacy protection, safe cloud storage, and search over encrypted information have all grown to be critical issues due to the rapid development of cloud services. The movement towards safe computation has received a lot of attention, particularly asymmetric scalar-product-preserving encryption (ASPE) and homomorphic encryption (HE). Although ASPE has the capacity to effectively encrypt and compare cipher texts, its reliance on the assumption that users can be completely trusted in the actual world and potential key leakage issues make it an impractical technique. In this research develop a content-based image retrieval system model that is security conscious and utilize the lightweight trapdoor model for verification, initially the input are collected from the standard repository and saved in an encrypted format. The image is encrypted using optimal chaotic map-based encryption, and the keys are produced on the user side to provide the image privacy and security. The image obtained after encryption is called as ciphered image. Hence for the purpose of image retrieval, the ciphered image is kept in the cloud. The relevant ciphered images are provided to the user whenever a search request is made by the query user using the trapdoors. Using an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters. The proposed hedge learner optimization is used to optimize the hybrid distance based clustering of images. Finally the cloud image that the user currently has been ciphered is decrypted using the owner's key.Based on the achievements at TP 80, the HLO Optimized Chaotic Encryption model achieve the MSE, PSNR, RMSE and SSIM values of 0.04, 61.67, 0.21 and 93.97 respectively. Similarly HLO Optimized Hybrid Distance based Clustering model achieves the F1 measure, precision and recall values during NOR 500 is 94.73%, 95.20% and 95.60% respectively.

Keywords: Encryption, decryption, trapdoor, chaotic map based encryption, hybrid distance based clustering, proposed hedge learner optimization

1. INTRODUCTION

Imaging technology has advanced quickly in the world, with examples including digital cameras, medical imaging equipment, smart phones, and more. As a result, digital image production substantially rises. There are a variety of useful Content-based Image Retrieval (CBIR) approaches that may be used to quickly find related images among a huge number of images. A typical image database, however, contains millions of images, some of which might be over 40 megabytes in size [1] [2]. Therefore, substantial processing and storage are typically needed for CBIR services. Because of these requirements, using a cloud server to outsource CBIR services is appealing. This eliminates the requirement for the image's owner to locally keep the image database and allows them to quickly obtain the desired images from the cloud server [3][4]. With the advent of big data and internet technology, the amount of image data is increasing quickly. It has become vital to figure out how to securely, promptly, and accurately extract useful content information. The use of visual features between the images being queried and the database images to determine visual similarity was made possible by content-based image retrieval technology [5], when compared to the early retrieval approach, which is mostly based on cross entropy loss [6]. An approximate similarity search strategy based on hashing database points is created in order to ensure the high collision probability between close points. Hashing has gained popularity as a contemporary approach for effective recovery of massive amounts of data [7] [8][3].

The conventional approaches for managing privacy in this situation [9][10] involve sensitive data is encrypted before being sent to a third party, and all computations are carried out on the client side. Numerous applications, particularly those operating online or on mobile devices and handling very large datasets like image repositories with CBIR services, are unable to handle this burden. It would be more practical to outsource calculations and carry out server-side operations on the encrypted data. The majority of the current solutions in this field are still impractical since they call for completely HE, which is still computationally prohibitively expensive [11]. While offering a good balance between security, privacy, and usability [12], partial homomorphic encryption techniques [13], [14], [15], [16] and symmetric key solutions (or property-preserving schemes) that support specific search patterns [17], [18], [19] are intriguing alternatives that produce more beneficial results. Users regularly upload image data to the cloud for processing and archiving as a result. Even though it offers significant convenience, this poses a serious security risk. Data that has been outsourced to the cloud is no longer directly under the owner's physical control, making it open to attack from outside hackers or "honest-but-curious" cloud service providers (CSP), as well as the possibility of abuse or leakage. Sensitive images must be encrypted before being transferred to clouds in order to safeguard users' privacy and improve data confidentiality, but this can make some typical cloud functions, such image retrieval, challenging [20] [21]. In the realm of image retrieval, CBIR has a lot of promise its distinguishing characteristic is the automatic comparison of the distance between features after extracting various image attribute [22]. However, the unpredictability introduced by the encryption process makes it impossible to retain the distance between image characteristics after the image has been encrypted, which makes the CBIR approach difficult to use [23].

Long-term solutions to this problem may be found in machine learning [11][23], which is a promising method. Machine learning has recently seen the introduction of some significant, cutting-edge new methodologies. With the use of deep architectures made up of numerous non-linear transformations, a family of ML algorithms known as deep learning which primary goal is to Model high-level abstractions in data. the deep architecture of the human brain's structure and the manner in which it transforms and represents information to carry out its functions, is similar to how deep learning operates [14][15]. Traditional machine learning techniques, on the other hand, frequently use "shallow" architectures.

The main aim of the research is to develop a content-based image retrieval system model that is security conscious and utilize the lightweight trapdoor model for verification, in the first step the data is collect from the standard repository, and saved in an encrypted format. The image is encrypted using optimal chaotic map-based encryption, and the keys are produced on the user side to provide the image privacy and security. The image obtained after encryption is called as ciphered image. Hence for the purpose of image retrieval, the ciphered image is kept in the cloud. The relevant ciphered images are provided to the user whenever a search request is made by the query user using the trapdoors. Using an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters. The proposed hedge learner optimization is used to optimize the hybrid distance based clustering of images. Finally the cloud image that the user currently has been ciphered is decrypted using the owner's key.

- ***Hedge learner optimization***: HLO is created by the typical hybridization of teaching learner and hedge search optimization. The hedge's behaviour involves searching food by reaching the global optima hence to enhance the searching speed the fitness of the teaching learner optimization is therefore hybridized with the hedge optimization to increase the searching capacity. This increases the searching speed by lowering the time complexity and delivers faster convergence.

According to its conceptual framework, the manuscript is divided into sections, with Section 2 describing recent works, their approaches, and their limitations. In Section 3, a model for content-based image retrieval utilizing the ensemble-proposed hedge learner optimization approach is presented. In Section 4, the hedge learner optimization is demonstrated, and Section 5 discusses the ultimate result.

2. MOTIVATION

The image is retrieved using a variety of methods using its color and texture attributes. Simple feature extraction techniques find it challenging to extract the high-level semantic information of the target image as a result, numerous different models are presented as a possible solution and to provide a deeper knowledge about the methods available in the existing works are analyzed and reviewed in the below section.

2.1Literature review

A novel bag-of-encrypted-words (BOEW) model was used by Zhihua Xia et al. [4] to construct a privacy-preserving CBIR system that offered good retrieval accuracy however, figuring out the database content from the received hash values proved computationally difficult for the client.Qing zhang 1 and yongyan [3] developed a deep ANN model to extract characteristics through sample training, which boosted the security of the image's network transmission. The encrypted data, however, covers the information included in the original images, making it difficult to obtain good outcomes.Yanyan xu and xiao zhao [23] developed a secure image retrieval method in a cloud environment that can reduce the redundant information, increase retrieval effectiveness, and ensure the security of the index. The randomness provided by the encryption process makes it challenging to maintain the gap between image components. A private preserving cloud-based image search system developed by Lan Zhang and Xiang Yang [1] was a first step towards useful cloud services which offered low-cost computing and communication with secure content-based large-scale image search and fine-grained access control, successfully safeguarding image privacy. The cloud finds it exceedingly challenging to keep the index structure preserved when dealing with large-scale images from different users.By merging the characteristics of color histogram features, R. Rani Saritha1 and Varghese Paul2 created a multi-feature image retrieval method [5]. This method generated a large data set for learning features and provided a good classification to handle the discovery of the successful content extraction, but this model encountered a number of issues because of the constraint imposed by the size of the database.FEI LIU1 et al. [6] developed an secure CBIR framework that carries out image retrieval on the cloud without requiring ongoing user input, this model achieved high CBIR accuracy. However, because of its high computational and memory costs, this approach is ineffective for real-world applications.Bernardo Ferreira et al.[7] developed a safe solution for outsourcing privacy-preserving storage and retrieval in big shared image repositories which exhibits good performance and scalability, but moving data storage to the Cloud introduces new security risks.Zhihua Xia et al. [9] developed a privacy-preserving image retrieval system where images are encrypted but may still be successfully recovered from the permutations of encrypted images that are similar to a query. This method increased security without affecting retrieval accuracy.

2.2Challenges

- However, the unpredictability introduced by the encryption process makes it impossible to retain the distance between image characteristics after the image has been encrypted, which makes the CBIR approach difficult to apply.
- CBIR commonly compares the distance between image features however applying cryptographic primitives to compare similarity across high dimensional vectors is difficult.
- However, it continues to struggle with the difficulties associated with freeing up mobile devices from onerous computational demands, such as data encryption, feature extraction, and image similarity scoring.
- Data outsourcing, especially to cloud computing infrastructures, seems to logically enable large-scale image storage and retrieval systems, but this also creates new problems for data privacy protection.
- Finding or recovering a suitable image from an archive is a challenging study topic due to the growth in the amount of shared and stored multimedia data[4][3][23].

3.PROPOSED CONTENT BASED IMAGE RETRIEVAL MODEL USING THE ENSEMBLE PROPOSED HEDGE LEARNER OPTIMIZATION

The primary aim of the research is to create a content-based image retrieval system that is security conscious and utilize the lightweight trapdoor for verification. Initially, the most important information required for image retrieval is collected from the standard repositories (Corel, European cities 1M, Labeled Faces in the Wild (LFW) Dataset, Flickr 27) and saved in an encrypted format. The image is encrypted using optimal chaotic map-based encryption, and the keys are produced on the user side to provide the image privacy and security. In the optimal chaotic map-based encryption, the image is shuffled and scrambled using a chaotic map's mathematical function to change the pixel value and location in order to encrypt data. The image obtained after encryption is called as ciphered image. Hence for the purpose of image retrieval, the ciphered image is kept in the cloud. The relevant ciphered imagesare provided to the user whenever a search request is made by the query user using the trapdoors (encrypted keywords). Using an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters. The proposed hedgelearner optimization, which is developed by standard hybridizing the sparrow search optimization (SSA) and teaching learning based optimization (TLBO), is used to optimize the hybrid distance based clustering of images. By using the hedge learner optimization, the sparrows' searching experience is improved. The intended output image is made possible by the optimization. The cloud image that the user currently has been ciphered is decrypted using the owner's key.

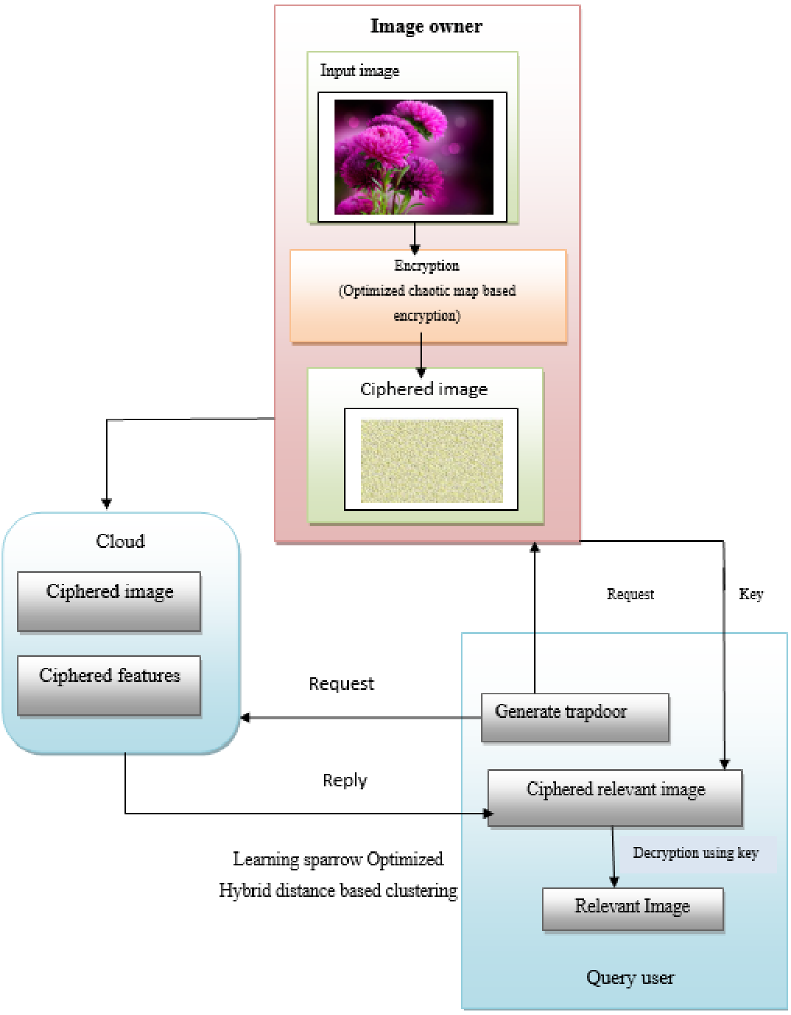


Figure 1: Architecture of the proposed CBIR model

3.1 Image owner

The owner of the data can safely outsource the images to the cloud server because encrypted images prevent information from being accessed by unauthorized users.

3.1.1 Input: The input for the content-based image retrieval system is obtained from the Corel, European cities 1M, Labeled Faces in the Wild (LFW) Dataset, Flickr 27 and is mathematically stated as follows:

$$T = \sum_{f=1}^{M} J_i + \sum_{f=1}^{M} K_i + \sum_{f=1}^{M} L_i + \sum_{f=1}^{M} M_i \quad (1)$$

In this instance, T refers to database, the value J_i , K_i *and* L_i represents the overall number of images stored in the database, which ranges from 1 to i .

3.1.2 Encryption

Encryption in the context of cryptography is the process of converting usable data into an unrecognizably different form to prevent unauthorized access. The image content's key properties, such as its high redundancy, size, capacity, and correlation between the bit pixels, necessitate the use of an encryption technique, with the main goal being the secure transport of the image. In other words, the useful real information is hidden by using an encryption technique to transfer the plain image into a cypher image. The encrypted image can then be delivered securely over the network so that no unauthorized user can decrypt the image.

3.1.3Optimized chaotic map based encryption

The problem is solved by chaos-based encryption methods, which generate uniformly spaced random keys that encode the visual information in the cipher images. But because these two scientific theories are closely related, they work well together to provide improved performance, high levels of security, and a variety of real-world applications, such as the production of pseudo-random numbers for use in stream ciphers, block ciphers, and other kinds of ciphers, etc. It is believed that chaotic systems are made up of a set of dynamical equations that change with time, which may be discrete or continuous.As these characteristics are comparable to the confusion and diffusion aspects of an effective cryptosystem, cryptosystems can be created using chaotic systems because of their specific qualities, including determinacy, ergodicity, and sensitivity to initial conditions.

Although there are several chaotic map-based image encryption techniques, there are three main components to the entire process or techniques. These three processes are carried out in any chaotic map-based image encryption method. These are many maps that are chaotic, confused, and diffused. Various systems are employed while developing these three processes, based on the demands and goals of each individual's design, such as the level of security, the need for key sensitivity, speed, etc. It is first necessary to analyze the behaviour of various chaotic maps in this situation. One or more maps must be chosen for use in encryption and decryption based on the user's requirements. The following action is to select a secret key that will be used to create the chaotic map's initial state and effective length under the assumption of brute force attack. So that the chaotic maps exhibit appropriate chaotic behaviour, initial parameters and constants must be determined. Following that, the chosen chaotic maps are ready to be used in the encryption process, which generates j_t, f_t after each iteration. Chaotic mapping functions are applied during the Confusion stage to reorganize the pixel values in the original image. To add further confusion to the resulting image, this technique may be done numerous times.

In the case of partial image encryption, this phase involves separating the bit planes and executing bit value confusion inside the planes. The diffusion stage is the following and last step to obtain the entire encrypted image. Each output pixel value from the confusion stage is XOR ed with the values of the chaotic function at this stage. To reach a higher security level, this step can be performed several times. The encrypted image is finally obtained and sent to the receiving side. In the decryption model, the procedure is repeated in reverse. The important difference is that everything is predetermined in this case, including the chaotic map, key, diffusion, and confusion mechanisms. The key needs to be regarded as being the same as that used in the encryption model. Afterwards, the same procedure must be used to determine the initial states and constants. The first diffusion step on the encrypted image must be performed in reverse order once the chaotic map is ready for usage. The confusion step's input comes from the diffusion step's output. The last decrypted image can then be recovered after the confusion stage is finished.

Two steps such as confusion and diffusion should be present in an encryption algorithm. There are often several rounds (iterations) before the confusion and diffusion processes start. The following is a mathematical notation for a cryptosystem:

$$B = \theta^{\alpha}\left(\phi^{\Omega}\left(J, M_{\kappa}\right), M_{\beta}\right)(2)$$

Where $J\ and\ M$ stand for the input plaintext image and the cipher text image, respectively, the confusion and diffusion function is denoted as $\theta\ and\ \phi$, confusion and diffusion secret keys are denoted as $M_K\ and\ M_\beta$, and the number of rounds for confusion and diffusion in the overall encryption is denoted by $\Omega\ and\ \alpha$. The general cryptosystem depicted in Fig.2 key space can be calculated as follows:

$$MG = \left(MG_f^{\Omega}.MG_{\beta}\right)^{\alpha} \ (3)$$

Where $MG_f\ and\ MG_\beta$ are the essential key spaces for the confusion and diffusion processes, respectively.

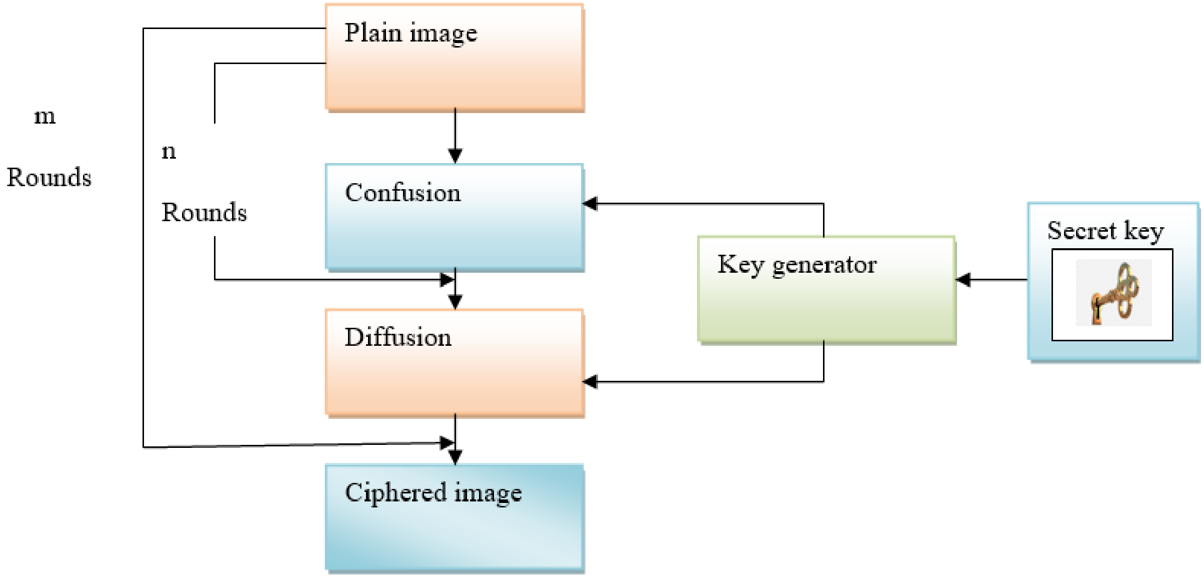


Figure 2: Architectural representation ofchaos based image encryption

3.2 Generation of trapdoor

3.2.1 Search request

After the data owner sends the encrypted images and secure index to the cloud server, our system is ready to provide services for content-based image search. The query descriptor is encrypted by a cryptosystem before the user requests the search service's permission. The data owner is still able to generate the trapdoor securely and covertly even after getting a vector made up of cipher messages. The user can obtain the encrypted trapdoor when the data owner delivers it to him again by using his own key to decipher the cipher text.

3.2.2 Retrieval

The secret key and query descriptor are combined to create the right trapdoor, which enables the cloud server to search the encrypted database. In order to stop attacks made possible by false trapdoors, the cloud server first determines if the false trapdoor was made by the data owner or not before allowing access to the necessary images. The service is promptly terminated if a false trapdoor is found by the cloud server. Because the retrieved data are cipher texts, the user must ask the data owner for the image key in the system's final step.

3.2.3 Trapdoor verification

Take extreme precaution to confirm the source of the trapdoor to avoid a fake door attacking the cloud server. If the trapdoor fails the test, the cloud server stops the search and gives the attacker nothing. The cloud server will check to see if the trapdoor adheres to the data owner's intended format or if the adversary changed it since the data owner constructs the secure index and trapdoor. It is feasible to discreetly conceal some information.

When creating the encrypted trapdoor for the user, the data owner chooses a positive integer δ and a non-prime positive integer $t = m \times g$ as the user's identification and extends the encrypted query descriptor $\{H(u1), H(u2), \ldots.. H(uv)\}$ to $v+2$ dimensional vectors $\{H(u1), \ldots.. H(uv), H(1), H(g)\}^F$ and multiplies the matrix v^{-1} by m. In the event when $\dot{U} = \left\{\dot{u}1, \dot{u}2, \ldots.\dot{u}v+2, \delta \times t\right\}^F$, the data owner will give the user $\left\{H\left(\dot{u}1\right), H\left(\dot{u}2\right), \ldots.. H\left(u\dot{v}+2\right)\right\}^F$ $\delta \times t$. After doing so, the user unlocks the trapdoor $\dot{U} = \left\{\dot{u}1, \dot{u}2, \ldots.\dot{u}v+2, \delta \times t\right\}^F$ by decrypting the cipher messages. Contrarily, when generating a safe index, we add an additional dimension to every non-leaf node that is as $\dot{tu} = \left\{\left(V^F\left(tu, -0.5 \| tu \|^2, \delta\right)^F\right)^F, -1\right\}^F$.

In this approach, the cloud servers verify whether an attacker had used the trapdoor before utilizing the secure index to look through the encrypted database. The following is a description of the verifying function in detail.

$$\dot{t}.\dot{U} = \left(\left(V^F\left(t, -0.5 \| t \|^2, \delta\right)^F\right)^F, -1\right)^F . \left(\left(mV^{-1}(u, 1, g)^F\right)^F, \delta \times t\right)^F \quad (3)$$

$$\dot{t}.\dot{U} = m\left(t^F u - 0.5 \| t \|^2 + \delta g\right) - \delta \times t \quad (4)$$

$$\dot{t}.\dot{U} = -0.5m\left(w^2(t, U) - \| U \|^2\right) + \delta(mg - t) \quad (5)$$

Because, $-1.5m \leq -0.5m\left(w^2(t, U) - \| U \|^2\right) \leq 0.5m)$, the cloud server determines that the trapdoor was not built by the data owner and terminates the service if the outcome of $\dot{t}.\dot{U}$ is not within $-1.5m$ *and* $0.5m$. Because the false trapdoor uses probabilistic encryption, the adversary is still unable to see the specifics of the original query descriptor, even though it successfully passes verification due to coordination with the cloud server.

The difficulty of analyzing trapdoors for system attack is increased when the trapdoor is perturbed with matrix and identity t, corresponding to a certain identity.

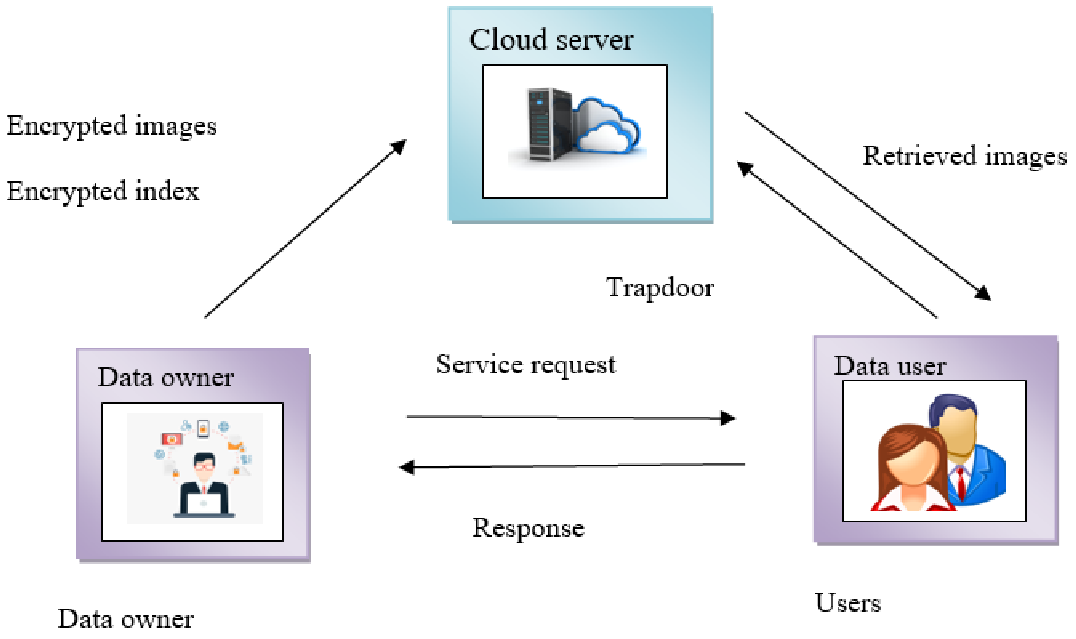


Figure 3: illustrative representation of trapdoor verifications

The cloud server disables the service if the result of $\dot{t}.\dot{U}$ is not found between-$-1.5m$ *and* $0.5m$ since it determines that the trapdoor was not built by the data owner at $-1.5m \leq -0.5m\left(w^{2}\left(t,U\right)-\| U \|^{2}\right) \leq 0.5m\right)$. As a result of the adversary's cooperation with the cloud server, the false trapdoor manages to pass verification, but because the trapdoor uses probabilistic encryption, it is still impossible for the adversary to learn the specifics of the original query descriptor.

The difficulty of analyzing trapdoors for system attack is increased when the trapdoor is perturbed with matrix and identity t, corresponding to a certain identity.

3.3 Hybrid distance based clustering methods

Using an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters.One of the well-known clustering algorithms for partitions is K-Means. A set of n items is divided into k clusters based on the input parameter k, the number of clusters, so that intra-cluster similarity is high but inter-cluster similarity is low. The definition of k centroids, one for each cluster, is the fundamental idea. These centroids should be strategically placed because different places have varied consequences. Therefore, it is preferable to situate them as far apart from one another as possible. Each point from a given data set is then taken as the next step, and it is then connected to the closest centroid. An early group age is complete once there are no outstanding points in the first step. k new centroids must now be calculated once more. Once we have these k new centroids, we must create a new link between the same data set points and the closest new centroid. There is currently a loop be created. Until no other alterations are made, the locations of the k centroid may gradually vary as a result of this loop. The algorithm's final goal is to minimize an objective function. The goal-oriented purpose is given as

$$K = \sum_{m=1}^{t}\sum_{n=1}^{tj}\left(\left\| p_m - q_n \right\|\right)^2 \quad (6)$$

The distance between p_m and q_n in Euclidean terms is $\left\| p_m - q_n \right\|$.

In the j^{th} cluster, tj is the total number of data points.

There are t cluster centers in total.

3.3.1 Distance measurement in K-mean clustering

By utilizing an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters.

3.3.2 Euclidean distance

The most popular distance measurement is the Euclidean distance.It is also known as the M_2 distance. If two points $c = (t_1, g_1)$ and $e = (t_2, g_2)$ have coordinate of $c\,and\,e$ respectively, the Euclidean distance between them is given by

$$TJ(c,e) = \sqrt{(t_1 - t_2)^2 + (g_1 - g_2)^2} \quad (7)$$

It is possible to generalize Equation 7 by defining the Euclidean distance between $d = (t_1, t_2, ..., t_u)$ and $f = (g_1, g_2, ..., g_u)$ as [3] if the points have n dimensions, such as d and f, rather than just two.

$$TJ(d, f) = \sqrt{(t_1 - g_1)^2 + (t_2 - g_2)^2 + (t_u - g_u)^2} \qquad (8)$$

$$\sqrt{\sum_{n=1}^{u} (t_n - g_n)^2} \quad (9)$$

3.3.3 Manhattan Distance

It is extremely comparable to Euclidean distance. According to Eq. 7, the city-block distance is the total of the distances along each dimension, whereas the Euclidean distance is the length of the shortest path between two places. This is the same as how far it would take to walk from one location to another in a city. Figure 4 illustrates how the Manhattan distance must move both horizontally and vertically since it cannot move with the points diagonally. The triangle inequality is satisfied by the city-block distance, making it a metric. Since the expression data are instantly subtracted from one another to calculate the Euclidean distance, it is important to ensure that they have been appropriately normalized.

It is also known as the M_1 distance. The Manhattan distance between $c = (t_1, g_1)$ and $e = (t_2, g_2)$ which is determined by $c\,and\,e$ if they are two points, is

$$AB(d, f) = |t_1 - t_2| + |g_1 - g_2| \qquad (10)$$

If a point has more than two dimensions, such as $d = (t_1, t_2, ..., t_u)$ and $f = (g_1, g_2, ..., g_u)$ equation 3 can be generalized by stating that the Manhattan distance between a and b is [3].

$$AB(d, f) = |t_1 - t_2| + |g_1 - g_2| + ... + |t_u - g_u|$$

$$= \sum_{n=1}^{u} |t_n - g_n| \qquad (11)$$

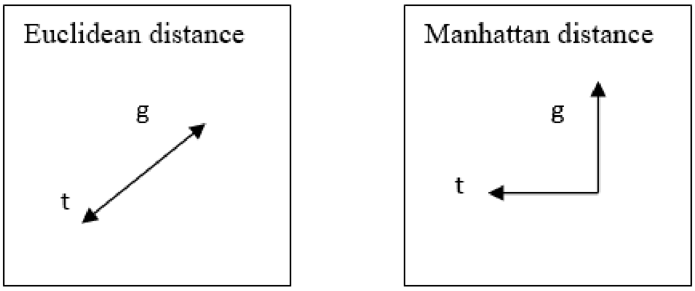


Figure 4: Difference between Euclidean and Manhattan Distance

4. PROPOSED HEDGE LEARNER OPTIMIZATION

In order to improve the efficiency of a clustering algorithm, the proposed hedge learner optimizationis used to optimize the hybrid distance based clustering of images. Hedge learner optimization (HLO) is a common hybridization of sparrow search optimization (SSO) [8] and teacher learner based optimization (TLBO) [2] .The hedge's behaviour involves searching food by reaching the global optima. The fitness of the teaching learner optimization is therefore hybridized with the hedge optimization to increase the searching capacity. This increases the searching speed by lowering the time complexity and delivers faster convergence.

4.1 Motivation

An efficient optimization method that mimics the foraging and anti-predation behaviors of hedges is the hedge search algorithm (HSA). Searching is the process of attentively or exhaustively looking into or over something in an effort to uncover or discover it [4]. The straightforward process of gathering food, either for immediate consumption or future storage, is known as hedge searching. There are many different species of gregarious birds that inhabit the hedges. They are found almost everywhere in the world and prefer to reside in areas where people live [3]. Hedges are important to the environment, but they are also important to human culture in many other ways. Their main sources of food are weeds and grain seeds. The common resident birds of the hedges are well known. When compared to many other small birds, the hedge is highly intelligent and has a powerful memory.

The teaching-learning process is the inspiration for TLBO, an algorithm that explains two fundamental modalities of learning through teachers and engaging with other learners. In this optimization technique, a population of students is taken into account, and the various subjects that are made available to them are considering as different factors of the optimization problem. The student's performance is equal to the optimization problem's "fitness" value. The teacher is seen as the population's best overall solution. The variables that compose the objective function of the given optimization problem are actually the design variables, and the optimal solution is determined by the objective function's best value. The two phases in which TLBO operates are the "Teacher phase" and the "Learner phase."

4.1.1 Mathematical model and algorithm

a) Initialization

In the simulation experiment, food must first be located using virtual sparrows. The following matrix can be used to show where sparrows are located.

$$F = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots\cdots & q_{1,t} \\ q_{2,1} & q_{2,2} & \cdots\cdots & q_{2,t} \\ . & . & \cdots\cdots & . \\ q_{h,1} & q_{h,2} & \cdots\cdots & q_{c,t} \end{bmatrix} \quad (12)$$

Hedge fitness can be represented by the following vector, where h represents the count of Hedge and d indicates the variable dimension to be optimized.

$$N_F = \begin{bmatrix} N([q_{1,1} & q_{1,2} & .... & q_{1,t}]) \\ N([q_{2,1} & q_{2,2} & ..... & q_{2,t}]) \\ . & . & ..... & . \\ N([q_{c,1} & q_{c,2} & ..... & q_{c,t}]) \end{bmatrix} \quad (13)$$

N_q stands for an individual's fitness value.

b) Solution based on self pipit

In HSA, the Hedge with the highest fitness value is given priority when looking for food. Strong Hedge is in charge of managing the movement of the entire population and seeking for food. In contrast to the weak hedge the strong hedge may find food in a wide variety of locations. The Strong Hedge position is indicated here as per and in each iteration.

$$F_{cm}^{t+1} = \begin{cases} F_{cm}^{t}.\exp\left(\dfrac{-c}{\lambda.iter_{\max}}\right) & if\ O_2 < ZS \\ F_{cm}^{t} + g.r & if\ O_2 \geq ZS \end{cases} \quad (14)$$

Where the current iteration $c = 1,2,....f$ is represented by t. F_{cm}^{t} denotes the c^{th} hedge at m^{th} dimension. $iter_{\max}$ is a constant and contains the most iterations. $\lambda \in (0,1]$is an arbitrary number. $(O_2 \in [0,1])$ and $ZS(ZS \in [0.5,1.0])$stand for alert value and safety threshold, respectively. g is a random variable that follows the normal distribution. The entire element inside the matrix, which has a dimension of $1 \times s$, has the value 1. A matrix B is created.

Where $O_2 < ZS$ denotes that there are no trappers present when the strong Hedge enters the wide search, and if $O_2 \geq ZS$ signifies that only a few of Hedge recognize the trapper and alertly fly all other Hedge to safe region.

c) Solution based on fittest depend Pipit

They designate the rule for the weak hedges; as previously stated, some weak hedges commonly observe strong hedges.Once weak Hedge learns strong Hedge has located a tasty meal, they quickly leave their current location and engage in combat for food. Strong Hedge will immediately supply the food if weak Hedge wins; otherwise, the rules will be followed. The position update formula as described in is for weak hedges.

$$F_{cm}^{t+1} = \begin{cases} g.\exp\left(\dfrac{F_{worst}^{t} - F_{cm}^{t}}{c^2}\right) & if\ c > y/2 \\ F_{x}^{t+1} + \left|F_{cm}^{t} - F_{x}^{t+1}\right| .J^{+}.r & otherwise \end{cases} \quad (15)$$

F_x is a representation of the strongest hedge in the best position. F_{worst}stands for the worst current location in the entire globe. If$c > y/2$, the weakest hedge with the lowest fitness value, represented by G, is starved. $J^{+} = J^{t}(JJ^{t})^{-1}$and -1 or 1 is assigned to each element inside matrix$1\times f$.

d) Exploration to exploitation

In the experiment simulation estimate that 10 to 20 percent of the population as a whole is aware of danger. In the population, a random starting location for a hedge is generated.

The importance of finding food in this situation is ranked highest for the hedge with the best fitness value. Strong Hedge is in charge of food finding and controlling population mobility.So compare to weakHedge the StrongHedge can search food in the broad range of places, in this case to obtain food for the low fitness weakHedge integrating the best T^{th} student fitness, hence now which can able to search food in the wide range by its attacking style with the help of fitness, which provides faster convergence and achieve high global search ability.

$$H = 0.5F_{cm}^{t+1} + 0.5A^{k}$$

$$H = 0.5\begin{cases} F_{best}^{t} + \delta.\left|F_{ab}^{t} - F_{best}^{t}\right| \\ F_{cm}^{t} + Y.\left(\dfrac{F_{ab}^{t} - F_{worst}^{T}}{\left(N_c - N_f\right) + \delta}\right) \end{cases} + \frac{\sum_{T=1}^{S} \dfrac{M^{T}(k)}{I^{T}}}{\sum_{T=1}^{S} \dfrac{1}{I^{T}}}; \qquad \frac{if\left(N_c > N_d\right)}{if\left(N_a = N_d\right)} \tag{16}$$

Where I^T stands for the student's fitness and S stands for the population's size. The weighted mean, which allowing students with excellent credentials more attention, should improve the performance of the upgraded TLBO algorithm.

δ denotes the control step size parameter, random integer denoted by $B \in [-1,1]$, has a variance of 1 and a mean value of 0 that follows the normal distribution. F_{best} represents the current, ideal location on the globe. While N_c stands for the current Hedge fitness value, the current global best and worst fitness values are denoted as N_f and N_d , respectively. For the lowest constant, use δ to avoid division by zero errors.

Where $N_c > N_d$ denotes that the Hedge is at the group's edge. F_{best} denotes the geographic centre of the population's designated safest area. In order to escape danger, the population in the region represented by $N_c = N_d$ is moving closer to its neighbor. Y denotes the direction in which the hedge is moving as well as the step size coefficient.

Table 1: Pseudo code for hedge learner optimization:

S.NO	Hedge learner optimization
1	Initialization: $F = \begin{bmatrix} q_{1,1} & q_{1,2} & \cdots\cdots & q_{1,t} \\ q_{2,1} & q_{2,2} & \cdots\cdots & q_{2,t} \\ . & . & \cdots\cdots & . \\ q_{h,1} & q_{h,2} & \cdots\cdots & q_{c,t} \end{bmatrix}$
2	Individual fitness value: $N_F = \begin{bmatrix} N([q_{1,1} & q_{1,2} & \cdots & q_{1,t}]) \\ N([q_{2,1} & q_{2,2} & \cdots & q_{2,t}]) \\ . & . & \cdots & . \\ N([q_{c,1} & q_{c,2} & \cdots & q_{c,t}]) \end{bmatrix}$

```
Solution based on strong hedge: $F_{cm}^{t+1} = \begin{cases} F_{cm}^{t}.\exp\left(\frac{-c}{\lambda.iter_{\max}}\right) & if\ O_2 < ZS \\ F_{cm}^{t} + g.r & if\ O_2 \geq ZS \end{cases}$
$if\ (O_2 < ZS)$
{
    no trappers present
}
else
{
    Trappers are nearby
}
Solution based on week hedge: $F_{cm}^{t+1} = \begin{cases} g.\exp\left(\frac{F_{worst}^{t} - F_{cm}^{t}}{c^2}\right) & if\ c > y/2 \\ F_x^{t+1} + \left|F_{cm}^{t} - F_x^{t+1}\right|.J^{+}.r & otherwise \end{cases}$
$if\ (c > y/2)$
{
    The weakest hedge with the lowest fitness value
}
else
{
    The strongest hedge with the highest fitness value
}
Exploration to exploitation:
    $H = 0.5\begin{cases} F_{best}^{t} + \delta.\left|F_{ab}^{t} - F_{best}^{t}\right| \\ F_{cm}^{t} + Y.\left(\frac{F_{ab}^{t} - F_{worst}^{T}}{(N_c - N_f) + \delta}\right) \end{cases} + \frac{\sum_{T=1}^{S} \frac{M^{T}(k)}{I^{T}}}{\sum_{T=1}^{S} \frac{1}{I^{T}}}; \quad \frac{if\ (N_c > N_d)}{if\ (N_a = N_d)}$
$if\ (N_c > N_d)$
{
    Hedge is at the group's edge.
}
else
{
    Hedge is not at the group’s edge.
}
if $(N_c = N_d)$
{
    Hedge is closer to its neighbor
}
else
{
    Hedge is closer to its neighbor
}
Termination
```

5. RESULT AND DISCUSSIONS

HLO optimized chaotic encryption model and HLO optimized hybrid distance based clustering model is proposed for the image retrieval model, and the model's accomplishments are justified by comparison to those methods.

5.1 Experimental setup

The experiment based on the content-based image retrieval model is conducted using Python on a Windows 10 computer with an internal memory of 8GB.

5.2 Dataset description

5.2.1 Corel

10 image concept groupings, each with 100 images. The images are split into 90 images for training and 10 images for testing for each concept group.

5.2.2 European cities 1M

The European Cities 1M dataset, which was crawled from Flickr using geographic queries to cover a window of each city centre, contains 909,940 geo-tagged images from 22 European cities.

5.2.3 Labeled Faces in the Wild (LFW)

A database of face images called Labeled Faces in the Wild (LFW) was created to examine the issue of unrestricted face identification. Researchers at the University of Massachusetts, Amherst, are responsible for creating and maintaining this database (particular references are listed in the section titled Acknowledgments). The Viola Jones face detector was used to locate 5,749 people in 13,233 images that were acquired from the internet. The dataset contains two or more distinct images of 1,680 of the individuals depicted. The original database includes three different kinds of "aligned" images in addition to four different sets of LFW images. In comparison to other image types, deep-funneled images, according to the researchers, gave better outcomes for the majority of face verification algorithms. So, this dataset is the deep-funneled version that was posted.

5.2.4 Flickr 27

Annotated logo data was acquired from Flickr to create the Flickr logos 27 dataset. Three image sets are used: There are 30 images for each of the 27 logo classes in the training set's 810 annotated images.

5.3Experimental result

This part contributes to the image retrieval model's analytical findings that were obtained using the HLO optimized chaotic encryption model. Figure illustrates the experimental results from the original image, encrypted image and the decrypted image is displayed in Figure 5.

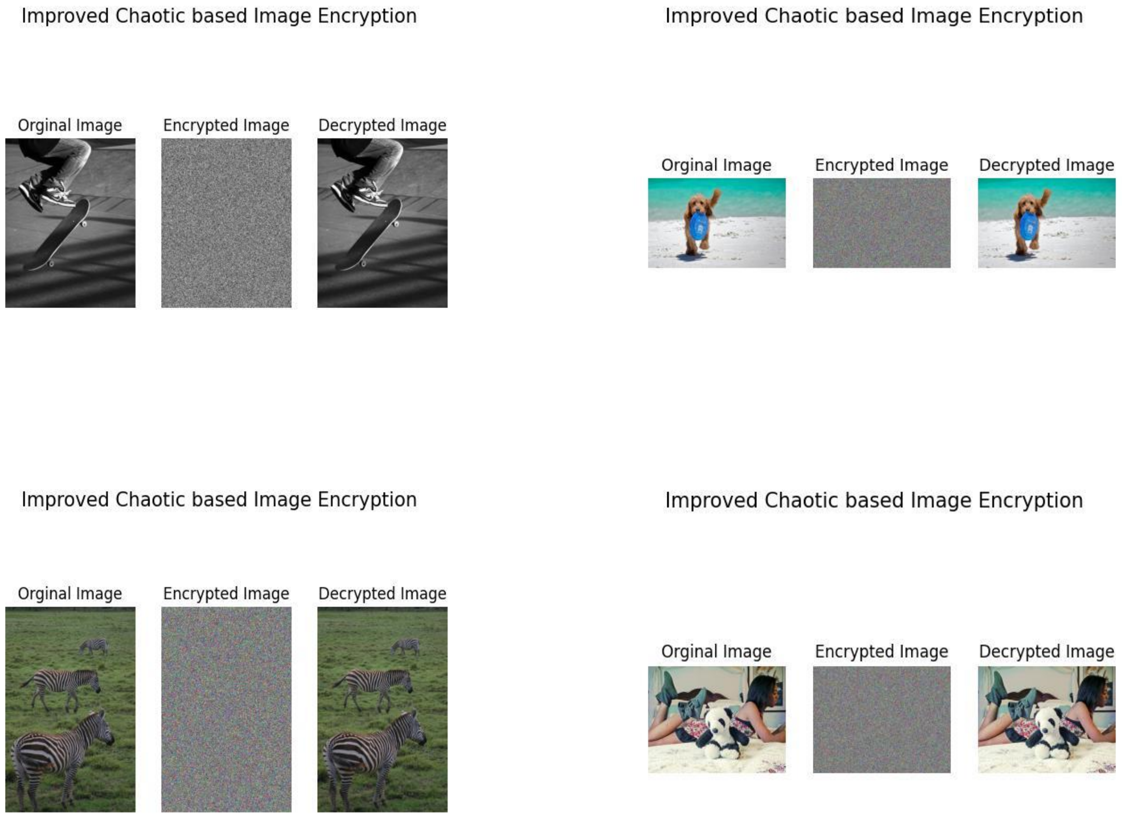


Figure 5: Experimental result obtained using HLO optimized chaotic encryption mode

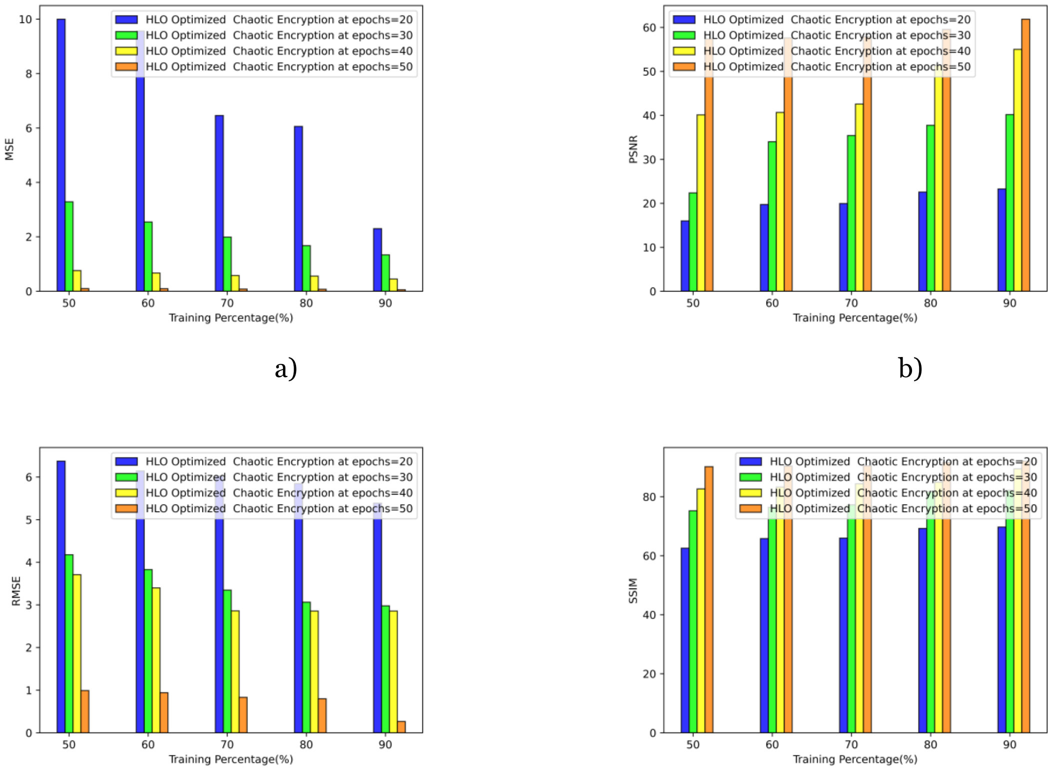
5.4Performance analysis based on encryption

The performance of the MSE, PSNR, RMSE, and SSIM chaotic encryption models is depict in Figure 6. Figure 6a) depicts the values that the HLO optimized chaotic encryption model produces with MSE epoch values 20, 30, 40 and 50 while keeping a training percentage (TP) of 80 the attain minimal error is 2.30, 1.34, 0.45 and 0.06.

Figure 6b) displays the results obtained utilizing the HLO-optimized chaotic encryption model with the epoch values of 20, 30, 40 and 50. The PSNR values were 23.27%, 40.18%, 55.03% and 61.89 % respectively.

Figure 6c) displays the results obtained utilizing the HLO-optimized chaotic encryption model with the epoch values of 20, 30, 40 and 50. The RMSE attains values with minimum errors of5.39, 2.98, 2.85 and 0.27 respectively.

Figure 6d) displays the results obtained utilizing the HLO-optimized chaotic encryption model with the epoch values of 20, 30, 40 and 50. The SSIM values were 69.73%, 82.18, 89.46% and 92.08% respectively.



a)

b)

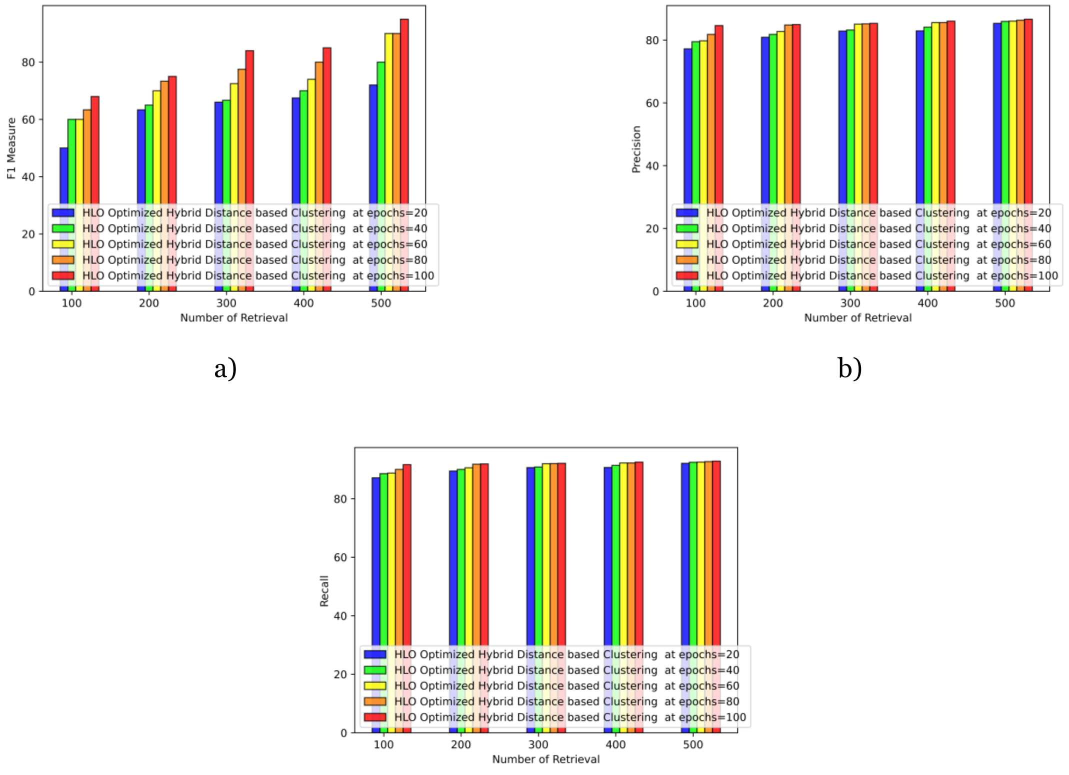
Figure 6: Analysis based on encryption a) MSE, b) PSNR, c) RMSE, d) SSIM

5.5Performance analysis for classification

The performance of the F1-score, precision, recall of HLO optimized hybrid distance based clustering model is depict in Figure 7. Figure 7a) shows the values that the HLO optimized hybrid distance based clustering model produces with F1-score epoch values 20, 40, 60, 80 and 100 while keeping a number of retrieval of 500 the attain values are 72%, 80%, 90%, 90% and 95% respectively.

Figure 7b) shows the findings obtained using the HLO optimized hybrid distance based clusteringmodel with the epoch values the obtained precision values were 85.33%, 85.95%, 86.05%, 86.34% and 86.67% respectively, with a NOR of 500.

Figure 7c) shows the findings obtained using the HLO optimized hybrid distance based clustering model with the epoch values the obtained recall values were 5.39, 2.98, 2.85 and 0.27 respectively, with a NOR of 500.



a) b)

c)

Figure 7: Performance analysis based on classification a) F1-score, b) precision, c) recall

5.6Comparative methods

The comparative analysis is conducted to illustrate the efficacy of the HLO-optimized chaotic encryption model, and the methods used for comparison arelogistic key encryption, XOR encryption, Lorenz key encryption, chaotic encryption, chaotic encryption with sparrow search optimization, chaotic encryption with teaching and learning based optimization.

The objective of the comparative analysis is to show how well the HLO optimized hybrid distance based clustering model performs well than other models which includes MLP classifier, decision tree, support vector machine, distance based clustering, SSA optimized distance based clustering, TLO optimized distance based clustering.

5.6.1 Comparative analysis based on encryption

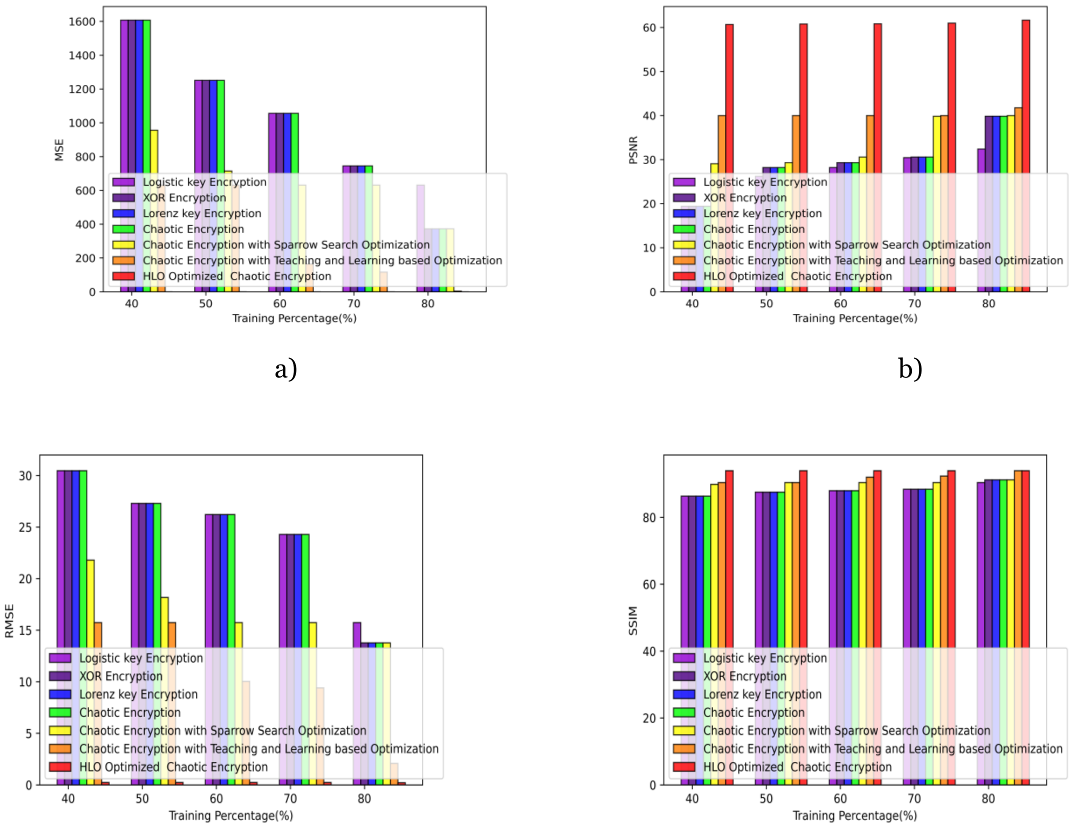
In accordance with the training %, Figure 8 shows the performance of the HLO-optimized chaotic encryption model by comparing the MSE, PSNR, RMSE, and SSIM.

The effectiveness of the HLO-optimized chaotic encryption model in image retrieval is shown in Figure 8a) .The HLO-optimized chaotic encryption outperforms the chaotic encryption with teaching and learning based optimization by the lowest error of 0.04 at a TP of 80.

The PSNR of the HLO-optimized chaotic encryption model in image retrieval is shown in Figure 8b). Chaotic encryption with teaching and learning based optimization is outperformed by HLO-optimized chaotic encryption model by 32.27%, and the HLO-optimized chaotic encryption model has a PSNR of 61.67% for a TP of 80.

The effectiveness of the HLO-optimized chaotic encryption model in image retrieval is shown in Figure 8c). The HLO-optimized chaotic encryption outperforms the chaotic encryption with teaching and learning based optimization by a minimum error of 0.21 at a TP of 80.

The effectiveness of the HLO-optimized chaotic encryption model in image retrieval is shown in Figure 8d). The HLO-optimized chaotic encryption outperforms the chaotic encryption with teaching and learning based optimization by 0.01% with a SSIM of 93.97% at a TP of 80.



a) b)

c)

Figure 8: Comparative analysis based on encryption a) MSE, b) PSNR, c) RMSE, d) SSIM

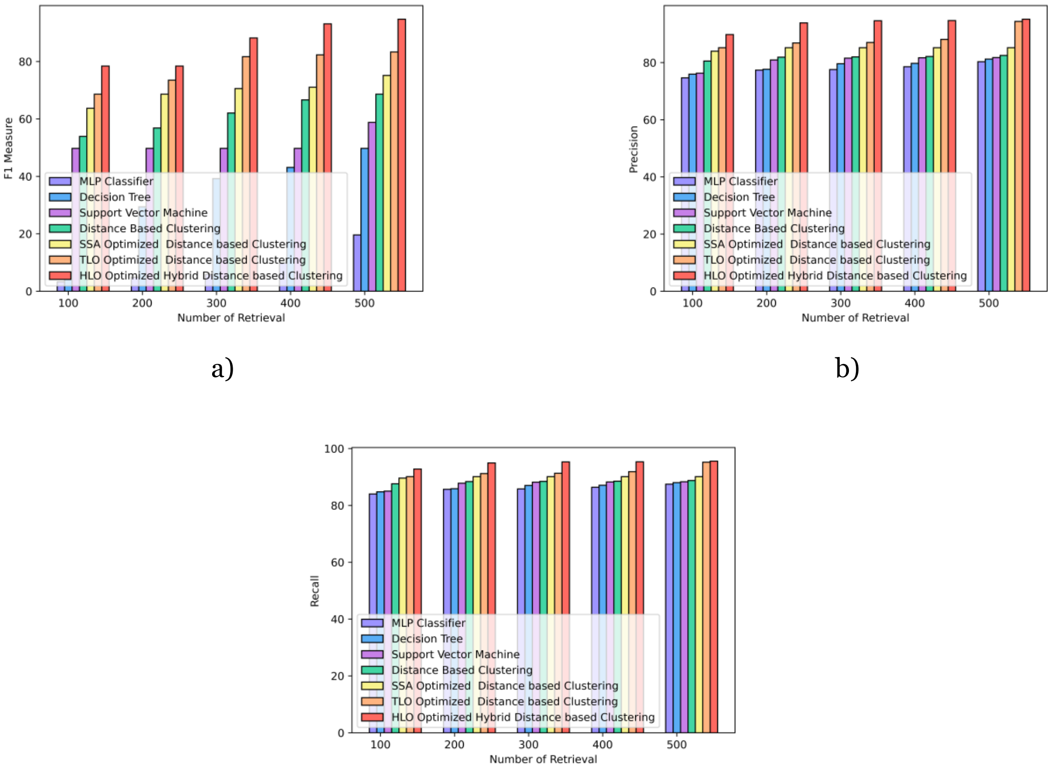
5.6.2 Comparative analysis based on classification

In accordance with the NOR 500, Figure 9 shows the performance of the HLO optimized hybrid distance based clustering model by comparing the F1 measure, recall and precision.

The effectiveness of the HLO optimized hybrid distance based clustering model in image retrieval is shown in Figure 9a). The HLO optimized hybrid distance based clustering model outperforms the TLO optimized distance based clusteringby 12.07% with a F1 score of 94.73% at a NOR of 500.

The precision of the HLO optimized hybrid distance based clustering model in image retrieval is shown in Figure 9b). TLO optimized distance based clusteringis outperformed by HLO optimized hybrid distance based clustering model by 0.83%, and the HLO optimized hybrid distance based clustering model has an precision of 95.20% for a NOR of 500.

The recall of the HLO optimized hybrid distance based clustering model in image retrieval is shown in Figure 9c). TLO optimized distance based clustering is outperformed by HLO optimized hybrid distance based clustering model by 0.42%, and the HLO optimized hybrid distance based clustering model has an precision of 95.60% for a NOR of 500.



a)

b)

c)

Figure 9: Comparative analysis based on classification a) F1-score, b) precision, c) recall

5.7Comparative discussion

Tables 1 and 2 analyze the results of the image retrieval models. The comparison in the table demonstrates that the suggested model achieves the best image encryption performance using MSE, PSNR, RMSE, and SSIM. Additionally, the results of the classification of the F1 measure, recall, and precision are displayed as below

Table 1: Comparative discussion forHLO-optimized chaotic encryption model

Model	TP 80			
	MSE	PSNR	RMSE	SSIM
Logistic key Encryption	631.05	32.40	15.74	90.41
XOR Encryption	372.59	39.86	13.77	91.21
Lorenz key Encryption	372.59	39.86	13.77	91.21
Chaotic Encryption	372.59	39.86	13.77	91.21
Chaotic Encryption with Sparrow Search Optimization	372.59	40.00	13.77	91.21
Chaotic Encryption with Teaching and Learning based Optimization	4.33	41.77	2.08	93.96
HLO Optimized Chaotic Encryption	0.04	61.67	0.21	93.97

Table 2: Comparative discussion forHLO optimized hybrid distance based clustering model

	NOR 500		
Models	F1-measure	Precision	Recall
MLP Classifier	19.60	80.33	87.47
Decision Tree	49.74	81.23	88.00
Support Vector Machine	58.80	81.78	88.32
Distance Based Clustering	68.60	82.51	88.75
SSA Optimized Distance based Clustering	75.13	85.22	90.14
TLO Optimized Distance based Clustering	83.30	94.41	95.20
HLO Optimized Hybrid Distance based Clustering	94.73	95.20	95.60

6. CONCLUSION

In this research develop a content-based image retrieval system model that is security conscious and utilize the lightweight trapdoor model for verification, initially the input are collected from the standard repository and saved in an encrypted format. The image is encrypted using optimal chaotic map-based encryption, and the keys are produced on the user side to provide the image privacy and security. The image obtained after encryption is called as ciphered image. Hence for the purpose of image retrieval, the ciphered image is kept in the cloud. The relevant ciphered images are provided to the user whenever a search request is made by the query user using the trapdoors. Using an efficient hybrid distance-based clustering method, the cloud's most pertinent ciphered images are chosen, and the user who requests them is given access to the relevant image clusters. The proposed hedge learner optimization is used to optimize the hybrid distance based clustering of images. Finally the cloud image that the user currently has been ciphered is decrypted using the owner's key. The proposed hedge learner optimization is used to optimize the hybrid distance based clustering of images. Finally the cloud image that the user currently has been ciphered is decrypted using the owner's key. Based on the achievements at TP 80, the HLO Optimized Chaotic Encryption model achieve the MSE, PSNR, RMSE and SSIM values of 0.04, 61.67, 0.21 and 93.97 respectively. Similarly HLO Optimized Hybrid Distance based Clustering model achieves the F1 measure, precision and recall values of 94.73%, 95.20% and 95.60% respectively.

Funding: This research did not receive any specific funding

Conflict of Interest: The authors declare no conflict of interest

Ethical approval: Not Applicable

Author Contribution: All authors have made substantial contributions to conception and design, revising the manuscript, and the final approval of the version to be published. Also, all authors agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

REFERENCES

[1] J. M. Lewin, R. E. Hendrick, C. J. D'Orsi, P. K. Isaacs, L. J. Moss, A. Karellas, G. A. Sisney, C. C. Kuni, and G. R. Cutter, "Comparison of full-field digital mammography with screen-film mammography for cancer detection: results of 4,945 paired examinations." Radiology, vol. 218, no. 3, pp. 873–80, 200

[2] J. Sivic and A. Zisserman, "Video Google: A text retrieval approach to object matching in videos," in Proc. ICCV, Nice, France, Oct. 2003, pp. 1470–1477.

[3] Zhang, Qing, Yong Yan, Yong Lin, and Yan Li. "Image Security Retrieval Based on Chaotic Algorithm and Deep Learning." IEEE Access 10 (2022): 67210-67218.

[4] Xia, Zhihua, Leqi Jiang, Dandan Liu, Lihua Lu, and Byeungwoo Jeon. "BOEW: A content-based image retrieval scheme using bag-of-encrypted-words in cloud computing." IEEE Transactions on Services Computing 15, no. 1 (2019): 202-214.

[5] Zhang, Lan, Taeho Jung, Kebin Liu, Xiang-Yang Li, Xuan Ding, Jiaxi Gu, and Yunhao Liu. "PIC: Enable large-scale privacy preserving content-based image search on cloud." IEEE Transactions on Parallel and Distributed Systems 28, no. 11 (2017): 3258-3271.

[6] Saritha, R. Rani, Varghese Paul, and P. Ganesh Kumar. "Content based image retrieval using deep learning process." Cluster Computing 22 (2019): 4187-4200.

[7] Liu, Fei, Yong Wang, Fan-Chuan Wang, Yong-Zheng Zhang, and Jie Lin. "Intelligent and secure content-based image retrieval for mobile users." IEEE Access 7 (2019): 119209-119222.

[8] J. Qin, H. Li, X. Xiang, Y. Tan, W. Pan, W. Pan, W. Ma, and N. N. Xiong, "An encrypted image retrieval method based on Harris corner optimization and LSH in cloud computing," IEEE Access, vol. 7, pp. 24626–24633,2019.

[9] Ferreira, Bernardo, Joao Rodrigues, Joao Leitao, and Henrique Domingos. "Practical privacy-preserving content-based retrieval in cloud image repositories." IEEE Transactions on Cloud Computing 7, no. 3 (2017): 784-798.

[10] F.-F. Li and P. Perona, "A Bayesian hierarchical model for learning natural scene categories," in Proc. CVPR, San Diego, CA, USA, Jun. 2005, pp. 524–531

[11]Xia, Zhihua, Lan Wang, Jian Tang, Neal N. Xiong, and Jian Weng. "A privacy-preserving image retrieval scheme using secure local binary pattern in cloud computing." IEEE Transactions on Network Science and Engineering 8, no. 1 (2020): 318-330.

[12] W.-T. Chu and F.-C. Chang, "A privacy-preserving bipartite graph matching framework for multimedia analysis and retrieval," in Proc. ICMR, Shanghai, China, Jun. 2015, pp. 243–250.

[13] C. S. Lu, "Homomorphic encryption-based secure sift for privacy preserving feature extraction," Proceedings of SPIE The International Society for Optical Engineering, vol. 7880, no. 2, pp. 788 005–17, 2011.

[14] L. Li, L. Feng, J. Wu, M.-X. Sun, and S.-L. Liu, "Exploiting global and local features for image retrieval," J. Central South Univ., vol. 25, no. 2, pp. 259–276, Feb. 2018,doi: 10.1007/s11771-018-3735-6.

[15] P. Ghosh and L. S. Davis, "Understanding center loss based network for image retrieval with few training data," in Proc. Eur. Conf. Comput. Vis., 2018, pp. 1–6

[16] Z. Yang, O. I. Raymond, W. Huang, Z. Liao, L. Zhu, and J. Long, "Scalable deep asymmetric hashing via unequal-dimensional embeddings for image similarity search," Neurocomputing, vol. 412, pp. 262–275, Oct. 2020

[17] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Process. Mag., vol. 30, no. 1, pp. 82–105, Jan. 2013.

[18] Z. Erkin, J. Li, A. P. O. S. Vermeeren, and H. de Ridder, "Privacypreserving emotion detection for crowd management," in Proc. AMT, Warsaw, Poland, 2014, pp. 359–370.

[19] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, Nov. 2012.

[20] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: A comparative study between homomorphic encryption and distancepreserving randomization," IEEE Access, vol. 2, pp. 125–141, 2014.

[21] Z. Xia, L. Jiang, D. Liu, L. Liu, and B. Jeon, "BOEW: A contentbased image retrieval scheme using bag-of-encrypted-words in cloud computing," IEEE Trans. Services Comput., to be published, doi: 10. 1109/TSC.2019.2927215

[22] Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Trans. Cloud Comput., vol. 6, no. 1, pp. 276–286, Mar. 2018

[23] Xu, Yanyan, Xiao Zhao, and Jiaying Gong. "A large-scale secure image retrieval method in cloud environment." IEEE Access 7 (2019): 160082-160090.