ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230922000954
Original scientific paper

Face Image Encryption Using Fuzzy K2DPCA and Chaotic MapReduce

Yunxiao LUO*, Ju LI

Abstract: As technology continues to advance, safeguarding personal privacy and information security has become increasingly critical. Facial image encryption algorithms involve encrypting and decrypting facial images to prevent unauthorized access and malicious use. Fuzzy computation is a practical solution for many decision problems in facial recognition encryption algorithms. To this end, this study proposes the use of fuzzy two-dimensional kernel principal component analysis for facial recognition and chaotic MapReduce for facial image encryption. The study introduces fuzzy membership functions to handle uncertainty in two-dimensional kernel principal component analysis. Experimental results indicated that the accuracy of the fusion fuzzy calculation and two-dimensional kernel principal component analysis method exceeded 75%, which was 13-37% higher than the comparison method. Furthermore, the proposed method combining chaotic systems and MapReduce has a uniform histogram distribution and runs 50% faster than the comparison method. Consequently, it is evident that the method proposed by the research institute is both feasible and efficient for safe facial image analysis.

Keywords: encryption algorithm; facial image recognition; fuzzy computing; two-dimensional kernel principal component analysis

1 INTRODUCTION

Face recognition technology, as a prominent area of research in computer vision, holds significant potential for both government and commercial applications. Safeguarding facial images for information security is of paramount importance [1]. Facial recognition technology serves as the cornerstone of facial image retrieval, with efficient extraction of facial recognition features being a top priority. Biometric identity authentication through face recognition offers advantages such as strong concealment, high operability, fast speed, convenience, low equipment costs, and non-intrusiveness [2, 3]. However, face recognition technology also faces challenges, including limitations imposed by self-perception and susceptibility to environmental influences. There are currently five main types of facial recognition technologies, namely geometric feature-based, algebraic feature-based, model-based, neural network-based, and 3D model-based methods [4, 5].

Traditional image protection methods primarily encompass digital watermarking technology and image encryption algorithms. Facial image encryption algorithms play a crucial role in preventing unauthorized access and malicious use through encryption and decryption of facial images [6, 7]. Existing image encryption algorithms are predominantly based on symmetric and asymmetric key encryption principles, in addition to specific image encryption methods, all employed to safeguard image data privacy and security. However, the combination of facial recognition encryption algorithms and fuzzy computing theory remains relatively uncommon in practical applications. This is partially due to the higher computational resource requirements and the complexity associated with algorithm implementation [8].

Nonetheless, there exists a wide array of decision problems that can be effectively addressed through fuzzy computation in practical facial recognition encryption algorithm applications. Fuzzy computing, as a theoretical model in computer science, is frequently utilized to tackle complex computational problems [9]. Its methodology involves distributing computing tasks across multiple resources to process information and subsequently merging the results, thereby enhancing computational efficiency and performance. By combining distributed computing resources with other technologies and methods, it becomes possible to improve problem-solving accuracy and efficiency, overcoming the limitations of traditional computing methodologies [10]. The specific approach involves distributing encryption algorithm tasks to multiple computing nodes for parallel encryption and decryption operations. This fully leverages computing resources, thereby enhancing the processing speed and performance of the encryption algorithm. In light of these considerations, this study aims to design an algorithm that integrates fuzzy computing with facial recognition encryption algorithms. It seeks to incorporate fuzzy computing concepts into the framework of the two-dimensional kernel principal component analysis algorithm, utilizing chaotic systems as encryption algorithms combined with the MapReduce program. The objective is to achieve more efficient and secure encryption operations. This research endeavors to enhance the accuracy of facial recognition, improve the security of facial image encryption, fortify the defenses of facial recognition technology, and expand its application scope. The research presents two innovative aspects: the fusion of fuzzy computing and two-dimensional kernel principal component analysis, as well as the amalgamation of chaotic systems and the MapReduce parallel computing framework.

This study is divided into four parts. The first part reviews current research findings. The second part describes the methods and design used in this study. The third part presents the experimental results and analysis of the research methods described in the second part. Finally, the fourth part summarizes the results of this study.

In the field of computer vision, protecting personal privacy and information security has become increasingly important with the continuous progress of technology. Bentafat et al. proposed a general privacy protection recognition framework to address significant privacy issues in large-scale video surveillance. The framework involved storing encrypted versions of suspect databases in cameras. Experimental results showed that for facial recognition with a database containing 100 suspects, the online computing time for the camera was 155 ms and for

the server was 34 ms, with a communication cost of only 12 KB. Similarly, for license plate recognition with a database of 3000 entries, the camera required 232 ms, the server required 75 ms, and the online communication cost 375 KB [11]. Sun et al. pointed out that near-infrared technology is capable of capturing high-definition and recognizable facial images at night. However, there are significant visual differences between near-infrared images and visible spectrum (VIS) images, and the technology itself is complex. To address the difficulty of learning cross-modal invariant features, Sun et al. proposed a cross-modal data gap decomposition method based on auxiliary modal methods. Extensive experiments were conducted on two commonly used datasets, CASIA NIR-VIS 2.0 and Oulu CASIA NIR-VIS, to evaluate this method. The experimental results indicated that this method outperformed the latest method [12]. To improve the efficiency of facial recognition, researchers such as Vanitha CN incorporated artificial intelligence technology, specifically an artificial intelligence facial recognition system. This technology extracted facial information from recorded images and matched it with facial information stored in a database. The study also utilized OpenCV for facial recognition, and the research results showed an accuracy of 94.8% for this method [13]. Experts like Hajarolasvadi N. designed a facial emotion recognition method based on special frames to enhance the efficiency of emotion recognition. This method utilized principal component analysis to capture feature frames in a single emotional video and reduced redundancy by mapping temporal changes to the feature space. The designed method was validated using multiple databases, and the experimental results demonstrated significantly higher efficiency in face recognition compared to existing baseline methods, as well as reduced computational time [14]. In order to improve the efficiency of retrieving information from different and large data sources, scholars such as Merlin NRG designed a method that integrates the MapReduce framework and the Jaya sine cosine algorithm. This method calculated the average value of the mapper data and transfers it to the reducer. Additionally, a parameterization-based method was employed to calculate similarity measures. The results showed that the designed method performed well in terms of accuracy and precision [15]. To enhance the security of online transactions, researchers such as Venkatesan R. developed a bidirectional authentication system that incorporates facial and proxy detection. Triple encryption technology was introduced to verify transmitted data. Moreover, nearly 130 feature points were embedded in the algorithm to improve the accuracy of face recognition. Experimental results demonstrated that the system designed by the research institute achieved improved accuracy and had a concise and user-friendly interface [16]. Traditional facial image encryption methods also have certain problems (as mentioned in reference [17]). Encryption technology based on compression encoding consumes more time and can impact the efficiency of the algorithm.

At the same time, there is a growing interest in fuzzy computing. Fuzzy computing is an algorithm that possesses unique advantages in addressing fuzzy problems, pattern recognition, fuzzy reasoning, and fuzzy modelling. By combining fuzzy computing with other technologies and methods, it is possible to overcome the limitations of traditional computing methods. To enhance the performance of existing local binary pattern operators, Chen et al. introduced the neighborhood weighted average operator. This operator took into account the strong correlation between neighboring pixel pairs. They expanded the traditional single-layer neighborhood template window to a double-layer neighborhood template window and calculated the weighted average of the double-layer neighborhood pixels in each direction. By comparing the symmetrically weighted average values of neighboring pixels around the central pixel, this algorithm effectively reduced computational complexity. Additionally, a feature fusion algorithm was proposed by leveraging the advantages of directional gradient histograms. Experimental results demonstrated that this algorithm exhibited stronger robustness under complex lighting conditions compared to many other state-of-the-art algorithms [18]. Boukezzoula et al. presented a calculation equation for the Bellman-Zadeh decision method based on intervals. The main objective was to maintain the flexibility of interval algorithms and interval reasoning. In this framework, decision-makers can choose the optimal solution within the specified decision criteria boundaries. This method considered risk decision criteria and can also incorporate other decision criteria in a similar manner. The Bellman-Zadeh decision problem, using membership functions, can be transformed into an interval arithmetic problem [19]. Kacher et al. proposed an algorithm for solving fully fuzzy multi-objective transportation problems using fuzzy harmonic averaging techniques. Firstly, they mathematically formalized FFMOTP and decomposed it into a three-level (lower, middle, and upper) multi-objective linear programming problem using fuzzy algorithms. Then, by employing fuzzy harmonic mean, the three-level multi-objective linear programming problem was transformed into a three-level single objective linear programming problem. The combination of fuzzy optimal solutions was obtained by solving these three levels of single objective linear programming problems [20]. Bharati et al. utilized interval-valued intuitionistic hesitation fuzzy sets to identify the limitations of previous optimization techniques research. They proposed a new optimization technique and developed a computational algorithm suitable for various real-life multi-objective optimization problems in engineering and management sectors. Additionally, a step-by-step calculation algorithm was constructed, which extended the application of fuzzy optimization technology and intuitionistic fuzzy optimization technology [21]. Delgoshaii A. and other experts designed a prediction method based on a comprehensive fuzzy algorithm to predict the innovative development mode of the supply chain. This method utilized the fuzzy weights of various factors in the support vector machine algorithm and implemented the model using Python. Experimental results demonstrated that this method outperformed the baseline method with smaller errors and higher prediction accuracy. It accurately predicted technological development in the green supply chain [22]. To enhance the obstacle avoidance capability of basketball robots, researchers like Shi developed a fuzzy dynamic obstacle avoidance algorithm based on multi-sensor data fusion technology. This algorithm involved

constructing a motion model of the robot and analyzing methods for controlling the robot's direction, speed, and position. A fuzzy obstacle avoidance strategy was then proposed and simulated for testing. The experimental results showed that the fuzzy obstacle avoidance strategy improved the obstacle avoidance ability of basketball robots. The tracking algorithm exhibited robustness and effectiveness [23]. However, existing fuzzy facial recognition methods (such as reference [24]) also have limitations in dealing with uncertainty.

In summary, experts have conducted research on facial image recognition algorithms and encryption algorithms, with a focus on improving the recognition accuracy and encryption security of the algorithms. Many experts have also conducted a lot of research on the integration of fuzzy computing theory with other fields of technology. However, the combination of facial recognition encryption algorithms and fuzzy computing theory is not very common. Nonetheless, there are numerous decision problems that can be solved by fuzzy computation in practical applications of facial recognition encryption algorithms. Therefore, designing an algorithm that combines fuzzy computation with facial recognition encryption algorithms holds certain value in handling fuzzy and incomplete information more effectively.

2 RESEARCH ON FACIAL IMAGE ENCRYPTION ALGORITHM BASED ON DISTRIBUTED FUZZY COMPUTING THEORY

This study improves upon the commonly used facial recognition algorithm, 2-D Kernel Principal Component Analysis (K2DPCA), by integrating fuzzy ideas and combining type data and sample distribution through relevant attribution functions. The nearest neighbor classifier is utilized for actual classification and recognition. This study comprehensively considers multiple factors such as data volume, communication, and encryption security. The encryption algorithm employed is a chaotic system, and the original image is encrypted using a highly sensitive chaotic system combined with the MapReduce program.

2.1 Research on Face Recognition Method Based on Fuzzy K2DPCA

Face recognition technology has a wide range of applications in different fields of society, and encryption algorithms play a very important role in face recognition technology. Facial images are first transformed into digital features for comparison and recognition using face recognition technology. Encryption algorithms in face recognition serve to protect the privacy and security of facial images. To enhance the performance of facial recognition encryption algorithms, the research proposes a method for facial recognition that integrates fuzzy computing and two-dimensional kernel principal component analysis. Additionally, a method that combines chaotic systems and the MapReduce parallel computing framework is designed for facial image encryption. The overall research process is illustrated in Fig. 1.

From Fig. 1, it can be seen that the first step of facial recognition and encryption methods is to introduce fuzzy computation based on 2D kernel principal component analysis (K2DPCA). The second step calculates membership, and the third step defines a fuzzy divergence matrix. The fourth step incorporates sample information into feature extraction, the fifth step extends the criteria for determining class separability to high-dimensional feature spaces, the sixth step selects the optimal projection axis, and the seventh step performs classification recognition.

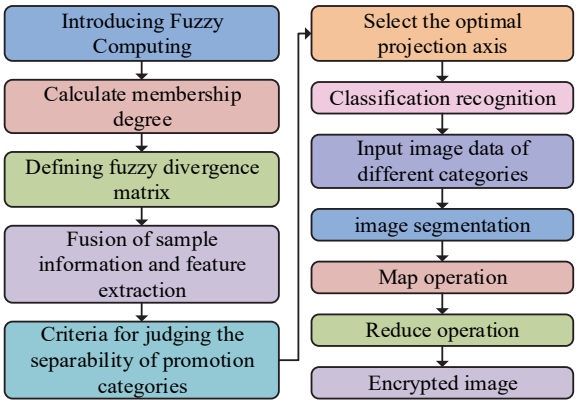


Figure 1 The overall process of research methods

Steps one to seven comprise the facial recognition portion. The eighth step involves inputting image data of different categories, the ninth step segments the image, the tenth step performs a Map operation, the eleventh step performs a Reduce operation, and the twelfth step outputs the encrypted image. Steps eight to twelve constitute the image encryption part. K2DPCA is a widely used method for facial recognition. Compared to traditional one-dimensional Principal Component Analysis (PCA), K2DPCA preserves the two-dimensional structure of the original image, better retains spatial information in facial images, and exhibits higher computational efficiency when processing large-scale data. However, its computational complexity remains relatively high [25]. This may pose a challenge in situations that demand rapid processing, such as facial recognition. Furthermore, K2DPCA solely selects feature vectors corresponding to relatively large feature values as the optimal projection axis, discarding some facial information that aids discrimination. As a result, the accuracy of projection axis selection decreases, leading to suboptimal problems [26]. In response to the difficulty of precise classification and the issue of edge categories involved in the application of K2DPCA technology in facial recognition, this study first integrates fuzzy thinking into K2DPCA, and then combines the type data of samples with their distribution through relevant attribution functions, integrating them at the feature extraction stage; Afterwards, the classification differentiation criteria for the samples in high-dimensional space will be set; Finally, the nearest neighbor classifier is used for actual classification and recognition. The K2DPCA method can map face image data with nonlinearity and non-separability into a high-dimensional feature space. It constructs the optimal hyperplane in this space to achieve linear separability. When introducing fuzzy concepts into K2DPCA, the class center in the high-dimensional feature space and the membership of samples in the class are calculated using the fuzzy K-nearest neighbor algorithm. Subsequently, the fuzzy divergence matrix in the high-dimensional feature space is defined, and the obtained information is

incorporated into facial feature extraction. The calculation of fuzzy membership is a key aspect of fuzzy set theory, elucidating the strength of the relationship between elements and fuzzy set members. Common methods for calculating fuzzy membership include the maximum membership method and the average membership method. The calculation process of the maximum membership method is depicted in Eq. (1).

$$u(\partial) = \max\left\{\mu\Upsilon(\partial), \mu\Omega(\partial), ..., \mu\Gamma(\partial)\right\} \tag{1}$$

In Eq. (1), Υ, Ω, and Γ are all fuzzy sets, $u(\partial)$ represents the maximum membership, ∂ represents the element, $\mu\Omega(\partial)$ represents the degree of the membership of the element ∂ in the fuzzy set Ω, and $\mu\Gamma(\partial)$ represents the degree of the membership of the element ∂ in the fuzzy set Γ. The calculation process of the average membership method is shown in Eq. (2).

$$\overline{u}(\partial) = \left(\mu\Upsilon(\partial), \mu\Omega(\partial), ..., \mu\Gamma(\partial)\right) / \Pi \tag{2}$$

In Eq. (2), $\overline{u}(\partial)$ represents the average membership degree, and Π represents the number of fuzzy sets. Eq. (3) describes the membership function of the sample obtained based on the fuzzy K-nearest neighbor criterion [27].

$$\mu_{i(jk)} = \begin{cases} 0.49 \times (n_{i(jk)} / K) & i \in j \\ 0.51 + 0.49 \times (n_{i(jk)} / K) & i \in j \end{cases} \tag{3}$$

In Eq. (3), $\mu_{i(jk)}$ is the degree of dependence of the k sample of class j on class i, and $n_{i(jk)}$ is the number of samples belonging to class i among the K nearest neighbor samples of the k sample of class j. The membership matrix $\mu = \left[\mu_{i(jk)}\right]$ of the training sample can be obtained through calculation. Eq. (4) describes the sample mean of the i -class sample in the high-order feature space obtained through the fuzzy mean calculation equation.

$$Fu_i = \frac{\sum_{j=1}^{c}\sum_{k=1}^{n_j} \mu_{i(jk)}^m \varphi(A_j^k)}{\sum_{j=1}^{c}\sum_{k=1}^{n_j} \mu_{i(jk)}^m} \tag{4}$$

In Eq. (4), $\varphi(A_j^k)$ is the total value of the sample in the high-order feature space, and m is the fuzzy index. Eq. (5) describes the fuzzy intra-class divergence matrix of the sample.

$$FS_w = \sum_{i=1}^{c}\sum_{j=1}^{c}\sum_{k=1}^{n_j} \mu_{i(jk)}^m (\varphi(A_j^k) - Fu_i)(\varphi(A_j^k) - Fu_i)^T \tag{5}$$

Eq. (6) describes the fuzzy intra-class divergence matrix of the sample.

$$FS_b = \sum_{i=1}^{c}\sum_{j=1}^{c}\sum_{k=1}^{n_j} \mu_{i(jk)}^m (Fu_i - Fu)(Fu_i - Fu)^T \tag{6}$$

In Eq. (6), Fu represents the mean of the population sample, and its expression is described by Eq. (7).

$$Fu = \frac{1}{N}\sum_{j=1}^{c}\sum_{k=1}^{n_j} \varphi(A_j^k) \tag{7}$$

In Eq. (7), N represents the total number of samples. Eq. (8) describes the fuzzy population divergence matrix of the sample.

$$FS_t = \sum_{i=1}^{c}\sum_{j=1}^{c}\sum_{k=1}^{n_j} \mu_{i(jk)}^m (\varphi(A_j^k) - Fu)(\varphi(A_j^k) - Fu)^T \tag{8}$$

Eq. (9) describes the relationship between the fuzzy inter-class divergence matrix, the fuzzy intra-class divergence matrix, and the fuzzy overall divergence matrix.

$$FS_t = FS_b + FS_w \tag{9}$$

In high-dimensional feature spaces, various facial samples can be linearly distinguished, however, in the original image space, this linear boundary may not exist [28]. Fig. 2 shows a three-dimensional spatial model. According to Fig. 2, it is assumed that the red, blue, and black lines represent the distribution characteristics of any two facial sample images in the space. In three-dimensional space, the red and black lines form two non-coplanar straight lines that can be linearly distinguished.

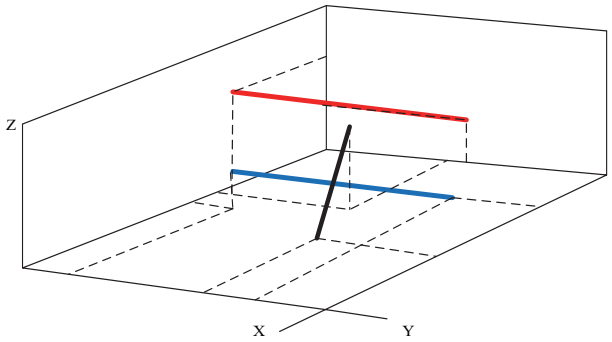


Figure 2 3D spatial model

After obtaining the optimal projection axis for the training sample, it can be used to create an optimal projection space. Fig. 3 shows the optimal projection axes and related projections obtained for two types of facial samples. It can be concluded that when facial image features can be represented in a high-dimensional feature matrix in the form of a single point, the distinction between the two samples can be determined by calculating the distance between two points in the two-dimensional space. The degree of this difference will be evaluated by the size of the distance and used as a criterion for determining the degree of category separation in high-dimensional space.

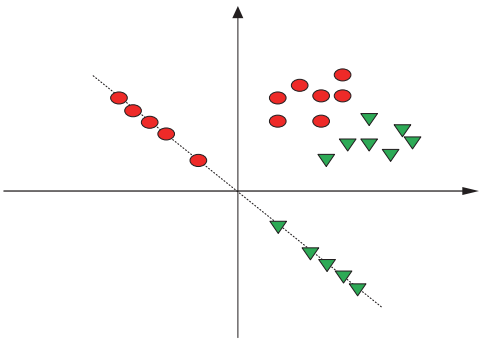


Figure 3 Optimal projection axis and correlation projection obtained from two types of facial samples

The judgment process is described by Eq. (10).

$$dist(\beta_1,\beta_2)=\left[(x_1-x_2)^2+(y_1-y_2)^2+(z_1-z_2)^2\right]^{\frac{1}{2}} \quad (10)$$

In Eq. (10), β_1 and β_2 are both points in the feature space model. If the dimension of the image vectors for any two facial samples is the same, which is 1 × 3, then the eigenvectors corresponding to their larger eigenvalues are w_1, w_2, and w_3. The feature vector that can make the intra-class divergence less than the inter-class divergence after projection is selected as the optimal projection axis, and this process is described by Eq. (11).

$$w_i^T FS_b w_i > w_i^T FS_w w_i \quad (11)$$

In Eq. (11), w_i is the optimal projection axis in the optimal projection space. You can choose feature vectors corresponding to smaller feature values as the optimal projection axis. This method not only extracts more facial recognition features that are helpful for recognition, but also solves the misclassification problem caused by the inter-class distance being smaller than the intra-class distance after using the nearest neighbor classifier to project the test sample. Eq. (12) describes the optimal discriminative features of faces.

$$Y=w_{FK2DPCA}^T\varphi(A) \quad (12)$$

$w_{FK2DPCA}^T$ is the optimal projection space. Finally, the nearest neighbor classifier is used for classification and recognition, which is described by Eq. (13).

$$dist(Y_p,Y_{\text{test}})=\min_{p=1}^{N} dist(Y_p,Y_{\text{test}}) \quad (13)$$

When solution Y_p belongs to class i sample, test sample Y_{test} is a class i facial image.

2.2 Construction of Image Encryption System Based on Mapreduce Parallel Computing Framework and Chaos System Fusion

Common algorithms, such as encryption based on matrix transformation or pixel displacement, use iteration limit or heuristic algorithms to perform matrix transformation on the image data matrix, that is, to disrupt the position of each pixel in the original image matrix to achieve the effect of encrypting the original image [29]. This ensures that the original image cannot be recognized after encryption, thereby achieving image encryption. Eq. (14) describes the commonly used transformation method, Arnold transformation [30].

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \quad (14)$$

In Eq. (14), x and y are any point (x, y) in the image matrix, while x' and y' are the transformed points. Based on Eq. (14), an image encryption algorithm can be implemented by transforming the points in the image data matrix and changing the pixel positions of the image data matrix. This process can be completed by limiting the number of iterations or using heuristic algorithms, as described by Eq. (15) [31].

$$\begin{bmatrix} x' \\ y' \end{bmatrix}=\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}(\text{mod } N) \quad (15)$$

In Eq. (15), $x, y \in \{0,1,2,...,N-1\}$, and N represents the order of the image matrix. It can be seen that encoding methods based on matrix transformation or pixel recombination mainly utilize mathematical transformation to reconstruct each pixel position in the original image matrix. This can scramble the pixel positions in the original image data matrix, achieving the scrambling effect. However, this approach has a significant drawback, as it only adjusts the pixel position in the original image without changing the grayscale value of the original image, no matter how complex or how many rounds of transformation this strategy undergoes [32]. Therefore, the histogram of the encoded image will not change, which makes this algorithm relatively weak in resisting attacks, resulting in low security [33].

In the field of image encryption, chaotic systems are highly sensitive to small changes in initial conditions and parameters, and have lower computational complexity compared to other encryption algorithms. Chaotic systems also possess multidimensional and unpredictable properties that can increase the difficulty of cracking the system. Furthermore, chaotic systems also have universality and can better represent sample data. There are six common image encryption algorithms: matrix transformation/pixel permutation-based, pseudo-random sequence-based, compression encoding-based, key image-based, secret segmentation and sharing-based, and chaotic system-based [34]. However, encryption methods based on matrix transformation/pixel permutation have weak attack resistance and poor security. The method based on pseudo-random sequences has relatively simple operations and therefore, poor security. The method based on compression encoding is time-consuming and can affect the encryption efficiency of the algorithm. The traditional key image-based methods have the problem of poor security, while the improved methods have the problem of long encryption

time and low efficiency. Secret segmentation methods have a strong dependence on sub keys, and secret sharing methods also bring a significant burden to data transmission when addressing the shortcomings of secret segmentation methods [35, 36]. Chaotic systems are sensitive to initial conditions, and image encryption systems are also sensitive to key images. Therefore, applying chaotic systems to image encryption systems is advantageous. Fig. 4 shows the encryption process of the chaotic system. It can be seen that all image data undergoes specific operations with the set generated by the chaotic system, transforming the original image information into new values similar to noise signals, thereby achieving the purpose of image encryption. The decryption process is the opposite. First, under the same initial conditions, a chaotic system is used to generate the same initial sequence set, and then the encrypted image information undergoes opposite operations with the set. This way, the noise-like signal that is added can be removed, and the final dataset obtained is the original image data.

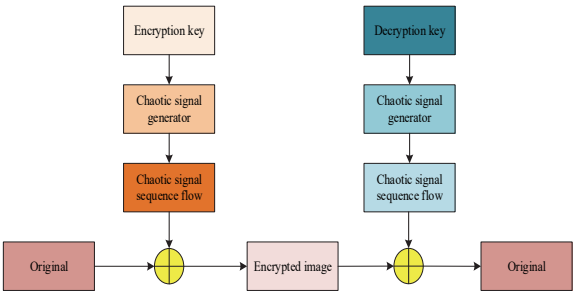


Figure 4 Chaotic system encryption process

Eq. (16) describes the encryption process based on chaotic systems.

$$X_{n+1} = \mu^* X_n (1 - X_n) \tag{16}$$

In Eq. (16), μ^* is used as a constant parameter to control chaotic behavior, X_n represents the current state value, and X_{n+1} represents the next state value. Taking into account multiple factors such as data volume, communication, and encryption security, this study has decided to use chaotic systems as encryption algorithms.

This study utilizes the MapReduce program and a highly sensitive chaotic system to encrypt original images. MapReduce, a programming model for processing large-scale data, can be decomposed into smaller sub-tasks, facilitating parallel processing when facing heavy tasks. MapReduce establishes distributed servers to run various tasks in parallel and manages data transmission within the system. MapReduce has scalability and fault tolerance and can leverage its advantages in multithreading, such as large-scale image data encryption. The core advantage of the MapReduce parallel computing framework is its ability to expand data processing on multiple computing nodes without modifying the corresponding program for each node, greatly reducing the time spent on updates. MapReduce comprises the Map stage and the Reduce stage. The Map stage divides input data into independent blocks and processes them in parallel, generating a set of key-value pairs for each block. The Reduce stage processes all key-value pairs output by the Map stage, aggregating and processing all values corresponding to the same key by the same Reduce task. Fig. 5 depicts the entire MapReduce system structure. It shows that data are first segmented and a map is established for them; then, the data are sorted in the map and split from memory to disk; the data is read out from the disk and run in memory, and then stored again on the disk; finally, a reduce integration operation is performed on all results to obtain the output.

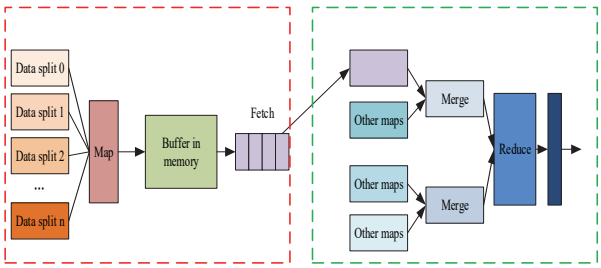


Figure 5 MapReduce system structure

The MapReduce model simplifies parallel processing of large amounts of data, allowing developers to focus on the task itself rather than worrying about the complex details of distributed systems. Ordinary image encryption programs require a high level of security, ensuring that encrypted images are highly sensitive to changes in key data, thereby increasing the difficulty of cracking encrypted images. Therefore, this program is suitable for encrypting original images using chaotic systems that are highly sensitive to keys. Based on the characteristics of image data and image encryption, this study chose the MapReduce parallel computing framework and chaotic system to execute the computational process of distributed image encryption, which is highly suitable and efficient. Fig. 6 shows the architecture of an image encryption system based on the MapReduce parallel computing framework and chaotic system. It reveals that the image segmentation algorithm is first applied to partition the original image, which presets the initialization stage of the Map operation. Then, a chaotic system iteratively calculates each segmented sub-image, followed by a Map operation where each node independently completes its own task. Finally, the results of all Map operations are summarized, and a Reduce operation is performed to obtain the final encrypted image.

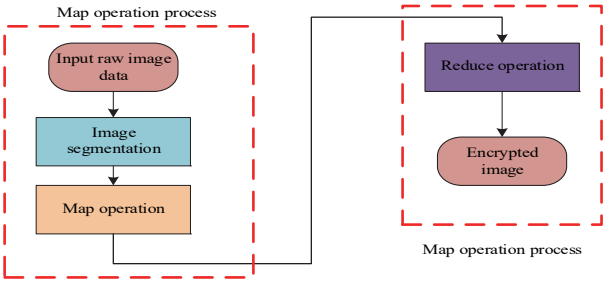


Figure 6 Encryption system architecture

3 EXPERIMENTAL RESULTS AND ANALYSIS OF ALGORITHM PERFORMANCE DETECTION

This experiment is divided into two stages. Firstly, the K2DPCA algorithm based on fuzzy computing theory was tested for its recognition performance in facial images.

PCA, two-dimensional principal component analysis (2DPCA), and K2DPCA were selected as comparative experimental subjects, and experiments were conducted on facial image databases Olivetti Research Laboratory (ORL) and YALE, respectively. Secondly, experiments were conducted on the algorithm's facial image encryption performance and security performance, and images from the image set were randomly selected as encryption objects.

3.1 Experimental Results and Analysis of Facial Recognition Performance Detection

In order to evaluate the recognition performance of the K2DPCA algorithm based on fuzzy computing theory for facial images, this study conducted experiments using PCA, two-dimensional principal component analysis (2DPCA), and K2DPCA as comparative experimental objects. The facial image libraries ORL and YALE were used for the experiments. The image dataset consisted of 2436 image data, with each image size of 12k and an image matrix size of 220 × 220. The original image resolution was 108500 × 81500 (approximately 8.84 billion pixels), with a PSD format file of 24GB and a Tiff format file of 3.9GB. The experimental platform comprised 1 Master node and 7 Worker nodes, where the Master node also served as a Worker node. The Master node was responsible for constructing the map node, receiving messages in the reduce stage, and integrating images. The Worker nodes were responsible for encrypting assigned subgraphs. To ensure comparability, 5 facial images of individuals were selected as training samples from each sample library in order, and the remaining samples were used for testing.

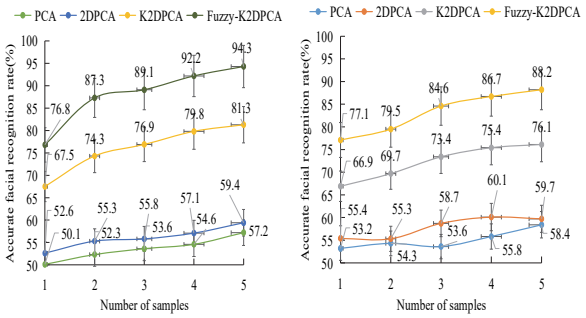


Figure 7 Comparison of best recognition performance

Fig. 7 presents a comparison of the best recognition performance of the four methods on different facial image sets. It can be observed that the Fuzzy K2DPCA method demonstrated greater stability and efficiency in overall performance compared to the three traditional facial recognition methods (PCA, 2DPCA, and K2DPCA). The overall recognition accuracy of the Fuzzy K2DPCA method was above 75%, with a maximum accuracy of 94.3%. By incorporating fuzzy membership information, the Fuzzy K2DPCA method effectively integrated category and distribution information into the feature extraction process, addressing edge category and hard classification problems encountered in face recognition. Additionally, through the establishment of classification separation criteria for high-dimensional feature spaces, the Fuzzy K2DPCA method achieved direct dimensionality reduction of the original samples. Ultimately, the optimal projection axis was selected based on projected feature vectors with inter-class divergence greater than intra-class divergence, allowing feature vectors corresponding to smaller non-zero eigenvalues to participate in the selection process.

Tab. 1 displays the average recognition accuracy of the four methods on different facial image sets. It is evident that the K2DPCA algorithm combined with fuzzy computing theory exhibited significantly higher recognition accuracy compared to the other three comparative algorithms on these two image sets. As the number of samples increased, this algorithm showed a maximum improvement in recognition accuracy of 18 percentage points, with an initial recognition accuracy above 75% to 25 percentage points higher than the other three comparative algorithms. The highest recognition accuracy achieved by this algorithm was 94.3%, surpassing other algorithms by 13 to 37 percentage points. The incorporation of fuzzy computing theory in facial image recognition has demonstrated favorable performance in recognition accuracy, consistent with reference [37], highlighting the benefits of integrating fuzzy computing theory in facial image recognition.

Table 1 Average recognition accuracy

ORL facial image set					
Algorithm Sample	1	2	3	4	5
PCA	50.1%	52.3%	53.6%	54.6%	57.2%
2DPCA	52.6%	55.3%	55.8%	57.1%	59.4%
K2DPCA	67.5%	74.3%	76.9%	79.8%	81.3%
Fuzzy-K2DPCA	76.8%	87.3%	89.1%	92.2%	94.3%
YALE facial image set					
Algorithm Sample	1	2	3	4	5
PCA	53.2%	54.3%	53.6%	55.8%	58.4%
2DPCA	55.4%	55.3%	58.7%	60.1%	59.7%
K2DPCA	66.9%	69.7%	73.4%	75.4%	76.1%
Fuzzy-K2DPCA	77.1%	79.5%	84.6%	86.7%	88.2%

3.2 Experimental and Result Analysis of Facial Image Encryption Performance Detection

To evaluate the performance of the facial image encryption method developed by the research institute, an experimental environment was first established. The platform consisted of one Master node and seven Worker nodes, each equipped with an Intel Core i5-5200u 2.2GHz dual-core/quad-threaded CPU, a 500GB hard disk, and 4GB of memory. The operating system used was Windows 10 (64 bit). Additionally, the Mapreduce MPI parallel library was configured on the machine, and the experiment's programs and data were stored in the same directory. To visually demonstrate the changes before and after applying the encryption algorithm to facial images, random images from the dataset were selected for experimentation. Fig. 8 presents a comparison between the original and encrypted images. It is evident that the clear image prior to encryption displayed uniformly distributed noise after being encrypted by the algorithm [38]. The facial feature information in the original image was effectively concealed, reflecting the successful operation of the encryption algorithm.

(a) Before image encryption (b) After image encryption

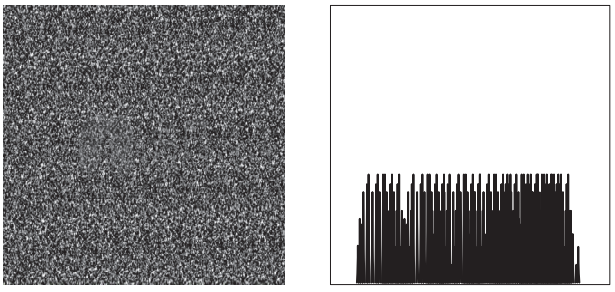
Figure 8 Comparison of original image and encrypted image

A security analysis of the image encryption was conducted by examining the image histogram, which displays the distribution of all data points. In image encryption, if the histogram exhibits uniformity, it indicates a better encryption effect. Fig. 9 depicts the histogram of the image processed using the proposed algorithm. The encrypted image shows high definition and discernible facial features, as evidenced by the non-uniform distribution of quality in the histogram.

(a) Before image encryption (b) Histogram of image before encryption

Figure 9 Original image and its histogram before processing

Fig. 10 presents the histogram of the image processed using the proposed algorithm. It can be observed that the encrypted image exhibits uniform noise, making it impossible to discern any facial feature information. The histogram reflects a uniform quality distribution, indicating a successful encryption effect. The MapReduce parallel computing framework has demonstrated excellent performance in facial image encryption, consistent with reference [38], which highlights the advantages of utilizing this framework in facial image encryption.



(a) After image encryption (b) Histogram of image after encryption

Figure 10 The processed original image and its histogram

Next, the real-time performance of the chaotic encryption algorithm proposed in this study was analyzed and compared with the Advanced Encryption Standard (AES) and Asymmetric Cryptographic Algorithm (RSA). Fig. 11 illustrates a comparison of the running time for encrypting and decrypting a large number of images using these three algorithms. It is evident that the chaotic encryption algorithm exhibits significantly shorter running times compared to the other two algorithms, both in the encryption and decryption processes. Although the running time increased for all three algorithms as the number of samples grew, the chaotic encryption algorithm performed exceptionally well [39]. For instance, when the number of samples reached 100, the chaotic encryption algorithm completed the task in only around 400 ms. Even when the sample size increased to 1000, the running time remained at approximately 800 ms, considerably lower than the other two algorithms.

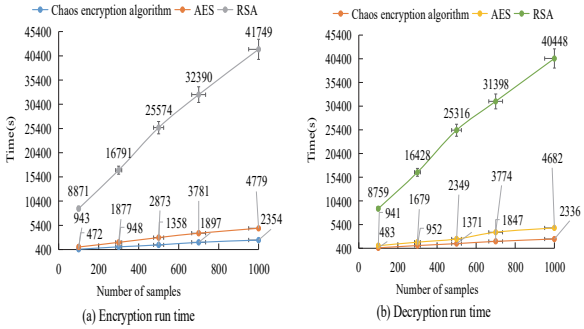


Figure 11 Comparison of running time

Tab. 2 shows the acceleration ratios of the encryption and decryption time of the chaotic encryption algorithm and AES algorithm. It can be seen that as the number of samples increased, the acceleration ratios between the two fluctuated around 0.5, and the amplitude was small, ranging from 0 to 0.03. The running time of the chaotic encryption algorithm was about half of that of the AES algorithm, and its performance was better. Chaos encryption algorithm has shown good performance in facial image encryption, which is consistent with reference [39], demonstrating the benefits of using chaos encryption algorithm in facial image encryption.

Table 2 Acceleration ratio of encryption and decryption time

Image collection size (pieces)	Chaos encryption algorithm	AES	Speed up
100	472	943	0.50
300	948	1877	0.51
500	1358	2873	0.47
700	1897	3781	0.50
1000	2354	4779	0.49

To better evaluate the performance of chaotic encryption algorithms, this study selected common facial recognition encryption algorithms for comparison. The comparative algorithms included Data Encryption Standard (DES) [40], Rivest Shamir Adleman algorithm (RSA) [41], and Elliptic Curve Cryptography (ECC) [42]. Additionally, all four algorithms underwent five image encryption tests, with the encrypted image data sourced from the ORL database. The comparison of recall rates for the four algorithms is presented in Tab. 3.

Table 3 Comparison of recall rates of four algorithms

Algorithm	Number of experiments				
	1	2	3	4	5
Chaos encryption algorithm	97.3%	96.5%	95.6%	96.8%	97.1%
DES	78.3%	73.5%	77.9%	75.2%	73.6%
RSA	80.1%	79.4%	78.6%	79.5%	81.7%
ECC	82.3%	83.7%	85.5%	84.9%	86.2%

Tab. 3 illustrates that the chaotic encryption algorithm achieved a maximum recall rate of 97.3% and a minimum value of 95.6%. The DES algorithm achieved a maximum recall rate of 78.3% and a minimum value of 73.5% [43-44]. The RSA algorithm achieved a maximum recall rate of 81.7% and a minimum value of 78.6% [45]. Lastly, the ECC algorithm achieved a maximum recall rate of 86.2% and a minimum value of 82.3%. It is evident that the chaotic encryption algorithm provided distinct advantages in terms of recall rate, thus indicating its superior performance [46].

4 CONCLUSION

Considering the multitude of decision problems that fuzzy computation can solve in practical applications of facial recognition encryption algorithms, this study aimed to effectively handle fuzzy and incomplete information. Building upon the two-dimensional kernel principal component analysis of common facial recognition algorithms, improvements were made by integrating fuzzy concepts. This was accomplished by combining type data of samples with their distribution using relevant attribution functions. Taking into account factors such as data volume, communication, and encryption security, a chaotic system was employed as the encryption algorithm. The MapReduce program was combined with a highly sensitive chaotic system to encrypt the original image. Experimental results demonstrated that the Fuzzy K2DPCA method exhibited greater stability and efficiency in overall performance compared to the three traditional face recognition methods, namely PCA, 2DPCA, and K2DPCA. The overall recognition accuracy surpassed 75%, with a maximum of 94.3%, which was 13 to 37 percentage points higher than the other algorithms. The algorithm successfully obscured facial feature information in the original image by transforming it into uniformly distributed noise following encryption. Analysis of the security performance of image encryption revealed that the encrypted image displayed uniform noise, making it impossible to discern facial features. The histogram demonstrated a consistent quality distribution, indicating a strong encryption effect. Furthermore, the real-time performance of the proposed chaotic encryption algorithm was analyzed. When the number of samples reached 100, the running time of the chaotic encryption algorithm was approximately 400ms. Even with a sample size of 1000, the running time remained around 800ms, significantly lower than the other two algorithms. The acceleration ratio between the chaotic encryption algorithm and AES fluctuated around 0.5, further highlighting the superior performance of the chaotic encryption algorithm. While this study effectively improved the encryption algorithm for facial image recognition, there are certain limitations to consider. Firstly, the impact of lighting on facial image recognition was not taken into account. Future research can analyze the influence of the external environment on facial image recognition to enhance accuracy. Secondly, for very large databases, this method may be limited by computational overhead and security. Future enhancements can explore approximate fuzzy techniques and hybrid encryption to further improve efficiency and robustness. Thirdly, there is still room for improvement in the real-time performance and security of chaotic systems. Future research can consider integrating heuristic algorithms into chaotic systems for optimization. Lastly, the classifier can be further optimized. Future research could explore alternative methods to optimize the nearest classifier or adopt new methods for facial classification.

Acknowledgements

Sponsored by Natural Science Foundation of Chongqing, China (Grant: CSTB2022NSCQ-MSX1632).

5 REFERENCES

[1] Chen, W. S., Ge, X., & Pan, B. (2022). A novel general kernel-based non-negative matrix factorisation approach for face recognition. *Connection Science*, *34*(1), 785-810. https://doi.org/10.1080/09540091.2021.1988904

[2] Yo, M. C., Chong, S. C., Wee, K. K., & Chong, L. Y. (2022). Sparse Representation with Principal Component Analysis in Face Recognition. *Journal of System and Management Sciences*, *12*(5), 57-72. https://doi.org/10.33168/JSMS.2022.0504

[3] Andrejevic, M. & Selwyn, N. (2020). Facial recognition technology in schools: Critical questions and concerns. *Learning, Media and Technology*, *45*(2), 115-128. https://doi.org/10.1080/17439884.2020.1686014

[4] Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2020). Facial-recognition algorithms: A literature review. *Medicine, Science and the Law*, *60*(2), 131-139. https://doi.org/10.1177/0025802419893168

[5] Ozdemir, D. & Ugur, M. E. (2021). Model proposal on the determination of student attendance in distance education with face recognition technology. *Turkish Online Journal of Distance Education*, *22*(1), 19-32. https://doi.org/10.17718/tojde.849872

[6] Krishnapriya, K. S., Albiero, V., Vangara, K., King, M. C., & Bowyer, K. W. (2020). Issues related to face recognition accuracy varying based on race and skin tone. *IEEE Transactions on Technology and Society*, *1*(1), 8-20. https://doi.org/10.1109/TTS.2020.2974996

[7] Gao, X., Mou, J., Banerjee, S., Cao, Y., Xiong, L., & Chen, X. (2022). An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), 1535-1551. https://doi.org/10.1016/j.jksuci.2022.01.017

[8] Ye, G., Liu, M., & Wu, M. (2022). Double image encryption algorithm based on compressive sensing and elliptic curve. *Alexandria engineering journal*, *61*(9), 6785-6795. https://doi.org/10.1016/j.aej.2021.12.023

[9] Fang, L., Yin, C., Zhou, L., Li, Y., Su, C., & Xia, J. (2020). A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine. *Information Sciences*, *507*, 143-160. https://doi.org/10.1016/j.ins.2019.08.020

[10] Yang, J. & Gao, H. (2020). Cultural Emperor Penguin Optimizer and Its Application for Face Recognition. *Mathematical Problems in Engineering*, *2020*(40), 1-16. https://doi.org/10.1155/2020/9579538

[11] Karanwal, S. (2021). Multi-scale neighbourhood based-tree binary pattern: a new feature descriptor for face recognition. *International Journal of Biometrics*, *13*(2), 322-342. https://doi.org/10.1504/ijbm.2021.114643

[12] Bentafat, E., Rathore, M. M., & Bakiras, S. (2021). Towards real-time privacy-preserving video surveillance. *Computer Communications*, *180*(10), 97-108. https://doi.org/10.1016/j.comcom.2021.09.009

[13] Sun, R., Shan, X., Zhang, H., & Gao, J. (2022). Data gap decomposed by auxiliary modality for NIR-VIS heterogeneous face recognition. *IET image processing*, *16*(1), 261-272.https://doi.org/10.1049/ipr2.12350

[14] Vanitha, C. N., Suwathika, S., Mathura, A., & Saranyadevi, P. (2021). Facial Recognition Processing Using Uniform Pattern Histogram with AI in Multimedia Applications. *Solid State Technology*, *64*(2), 788-798.

[15] Hajarolasvadi, N. & Demirel, H. (2020). Deep facial emotion recognition in video using eigenframes. *IET Image Processing*, *14*(14), 3536-3546. https://doi.org/10.1049/iet-ipr.2019.1566

[16] Merlin, N. R. G. & Vigilson, P. M. (2023). Efficient indexing and retrieval of patient information from the big data using MapReduce framework and optimisation. *Journal of Information Science*, *49*(2), 500-518. https://doi.org/10.1177/01655515211013708

[17] Venkatesan, R., Anni Princy, B., Ambeth Kumar, V. D., Raghuraman, M., Gupta, M. K., Kumar, A., & Khan, A. K. (2021). Secure online payment through facial recognition and proxy detection with the help of TripleDES encryption. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(8), 2195-2205. https://doi.org/10.1080/09720529.2021.2011096

[18] Liu, S., Li, C., & Hu, Q. (2021). Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE MultiMedia*, *29*(1), 74-84. https://doi.org/10.1109/MMUL.2021.3114589

[19] Chen, T., Gao, T., Li, S., Zhang, X., Cao, J., Yao, D., & Li, Y. (2021). A novel face recognition method based on fusion of LBP and HOG. *IET Image Processing*, *15*(14), 3559-3572. https://doi.org/10.1049/ipr2.12192

[20] Boukezzoula, R. & Coquin, D. (2020). A decision-making computational methodology for a class of type-2 fuzzy intervals: An interval-based approach. *Information Sciences*, *510*, 256-282. https://doi.org/10.1016/j.ins.2019.09.020

[21] Kacher, Y. & Singh, P. (2022). Fuzzy harmonic mean technique for solving fully fuzzy multi-objective transportation problem. *Journal of Computational Science*, *63*(9), 1-14. https://doi.org/10.1016/j.jocs.2022.101782

[22] Bharati, S. K. (2021). An Interval-Valued Intuitionistic Hesitant Fuzzy Methodology and Application. *New Generation Computing*, *39*(2), 377-407. https://doi.org/10.1007/s00354-021-00132-4

[23] Parameshachari, R. & Chandramouli, S. M. (2021). Building Enhanced Chaotic Map Encryption Method for Medical Information System. *Journal of System and Management Sciences*, *11*(1), 176-192. https://doi.org/10.33168/JSMS.2021.0111

[24] Delgoshaei, A., Beighizadeh, R., Arffin, M. K. A. B. M., Leman, Z. B., & Ali, A. (2023). Forecast Innovative Development Level in Green Supply Chains Using a Comprehensive Fuzzy Algorithm. *International Journal of Fuzzy Systems*, *25*(2), 880-895. https://doi.org/10.1007/s40815-022-01416-7

[25] Shi, F. & Hu, X. (2022). Fuzzy Dynamic Obstacle Avoidance Algorithm for Basketball Robot Based on Multi-Sensor Data Fusion Technology. *International Journal of Foundations of Computer Science*, *33*(6), 649-666. https://doi.org/10.1142/S0129054122420084

[26] Dirik, M. (2023). Optimized Anfis Model with Hybrid Metaheuristic Algorithms for Facial Emotion Recognition. *International Journal of Fuzzy Systems*, *25*(2), 485-496. https://doi.org/10.1007/s40815-022-01402-z

[27] Hao, M., Liu, G., & Xie, D. (2021). Hyperspectral face recognition with a spatial information fusion for local dynamic texture patterns and collaborative representation classifier. *IET Image Processing*, *15*(8), 1617-1628. https://doi.org/10.1049/ipr2.12131

[28] Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Hybrid face recognition under adverse conditions using appearance‐based and dynamic features of smile expression. *IET Biometrics*, *10*(1), 99-115. https://doi.org/10.1049/bme2.12006

[29] Zhang, G., Porikli, F.M., Sun, H., Sun, Q., Xia, G., & Zheng, Y. (2020). Cost-sensitive joint feature and dictionary learning for face recognition. *Neurocomputing*, *391*, 177-188. https://doi.org/10.1016/j.neucom.2020.01.101

[30] Ergin, S., Isik, S., & Gulmezoglu, M. B. (2021). Face Recognition by Using 2D Orthogonal Subspace Projections. *Traitement du Signal*, *38*(1), 51-60. https://doi.org/10.18280/TS.380105

[31] Lu, D. & Yan, L. (2021). Face Detection and Recognition Algorithm in Digital Image Based on Computer Vision Sensor. *Journal of Sensors*, *2021*(6), 4796768.1-4796768.16. https://doi.org/10.1155/2021/4796768

[32] Liu, Y. & Chen, J. (2021). Multi‐factor joint normalisation for face recognition in the wild. *IET Computer Vision*, *15*(6), 405-417. https://doi.org/10.1049/cvi2.12025

[33] Yaman, O., Tuncer, T., & Tasar, B. (2021). DES-Pat: A novel DES pattern-based propeller recognition method using underwater acoustical sounds. *Applied Acoustics*, *175*(4), 107859.1-107859.13. https://doi.org/10.1016/j.apacoust.2020.107859

[34] Deng, K., Peng, Z., & Zhu, W. (2020). A Discriminative Projection and Representation-Based Classification Framework for Face Recognition. *SIAM Journal on Imaging Sciences*, *13*(3), 1446-1466. https://doi.org/10.1137/19M1253873

[35] Saeed, M., Ahmad, M. R., & Rahman, A. U. (2022). Refined Pythagorean Fuzzy Sets: Properties, Set-Theoretic Operations and Axiomatic Results. *Journal of Computational and Cognitive Engineering*, *2*(1), 10-16. https://doi.org/10.47852/bonviewJCCE2023512225

[36] Zhong, H. & Li, G. (2022). Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling. *Multimedia Tools and Applications*, 81(17), 24757-24776.https://doi.org/10.1007/s11042-022-12479-x

[37] Gu, Z., Li, H., Khan, S., Deng, L., Du, X., Guizani, M., & Tian, Z. (2021). IEPSBP: a cost-efficient image encryption algorithm based on parallel chaotic system for green IoT. *IEEE Transactions on Green Communications and Networking*, *6*(1), 89-106. https://doi.org/10.1109/TGCN.2021.3095707

[38] Zheng, J. & Zeng, Q. (2022). An image encryption algorithm using a dynamic S-box and chaotic maps. *Applied Intelligence*, *52*(13), 15703-15717. https://doi.org/10.1007/s10489-022-03174-3

[39] Wu, M., Su, W., Chen, L., Pedrycz, W., & Hirota, K. (2020). Two-stage fuzzy fusion based-convolution neural network for dynamic emotion recognition. *IEEE Transactions on Affective Computing*, *13*(2), 805-817. https://doi.org/10.1109/TAFFC.2020.2966440

[40] Hu, L., Yang, S., Luo, X., Yuan, H., & Zhou, M. C. (2022). A Distributed Framework for Large-scale Protein-protein Interaction Data Analysis and Prediction Using MapReduce. *IEEE/CAA Journal of Automatica Sinica*, *9*(1), 160-172. https://doi.org/10.1109/JAS.2021.1004198

[41] Wu, T., Zhang, C., Chen, Y., Cui, M., Huang, H., Zhang, Z., & Qiu, K. (2021). Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission. *Optics Express*, *29*(3), 3669-3684. https://doi.org/10.1364/OE.416154

[42] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data encryption for Internet of Things applications based on catalan objects and two combinatorial structures. *IEEE Transactions on Reliability*, *70*(2), 819-830. https://doi.org/10.1109/TR.2020.3010973

[43] Yudistira, R. (2020). AES (Advanced Encryption Standard) and RSA (Rivest−Shamir−Adleman) Encryption on Digital Signature Document: A Literature Review. *International Journal of Information Technology and Business*, *2*(2), 26-29.

[44] Yin, S., Liu, J., & Teng, L. (2020). Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. *International Journal of Network Security*, *22*(3), 421-426. https://doi.org/10.6633/IJNS.202005 22(3).07

[45] Rajashekar, K. J., Ismail, C. B., Islam, M. T., & Bari, A. (2023). Dynamic load balancing in distributed storage systems using modified Whale optimization techniques. *Journal of System and Management Sciences*, *13*(1), 605-619. https://doi.org/10.33168/JSMS.2023.0130

[46] Zhang, L. L. & Kim, H. K. (2021). The Impacts of Customer Characteristics on Innovation Resistance in Using Face Recognition Payment Systems: An Empirical Study. *Journal of System and Management Sciences*, *11*(3), 101-118. https://doi.org/10.33168/JSMS.2021.0306

Contact information:

Yunxiao LUO
(Corresponding author)
Chongqing Open University & Chongqing Technology and Business Institute,
Chongqing, 401520, China
E-mail: luoyunxiao68@163.com

Ju LI
Chongqing Open University & Chongqing Technology and Business Institute,
Chongqing, 401520, China
E-mail: liju00130922@126.com