World Wide Web (2023) 26:1223–1241
https://doi.org/10.1007/s11280-022-01090-7

Web-based practical privacy-preserving distributed image storage for financial services in cloud computing

Cai Xiaohong[1] · Sun Yi[1] · Lin Zhaowen[1] · Muhammad Imran[2] · Yu Keping[3,4]

Received: 8 February 2022 / Revised: 31 May 2022 / Accepted: 25 July 2022 /
Published online: 4 August 2022

Abstract
With the development of multimedia technology and applications in the financial services industry, a large amount of multimedia image data related to financial services has been generated. For local users with limited resources including enterprises and individuals, it is a better choice to make full use of the rich storage capacity of the cloud. However, due to outsourcing the financial services image data to store on the cloud server, local users lose their direct control ability, which threatens the privacy of users. Although data security storage has attracted great attention from researchers, the protection of massive amounts of data, especially for financial services images, is brought to a new level with the advent of the era of artificial intelligence. In this paper, we focus on this issue and propose a lightweight data storage approach for privacy-preserving financial services images in the cloud. First, we use the EfficientDet neural network model to identify a large number of financial services images with sensitive data and classify the images. Then we perform different operations on the two types of images based on our proposed privacy-preserving financial services image storage architecture. Specifically, for privacy-sensitive financial services images, we use the privacy-preserving scheme we proposed to store the privacy parts on different servers, and directly outsource the storage of the remaining images without sensitive information. The experimental results show that our scheme achieves $2x - 5x$ lower than some popular image encryption schemes on time consumption, and simultaneously protects the security of images. In particular, our scheme shows more excellent performance when it comes to storing a large number of financial services multimedia images.

Keywords Privacy-preserving · Image storage · Cloud computing · Deep learning

This article belongs to the Topical Collection: Special Issue on *Web-based Intelligent Financial Services.* Guest Editors: Hong-Ning Dai, Xiaohui Haoran, and Miguel Martinez

✉ Sun Yi
sybupt@bupt.edu.cn

✉ Yu Keping
keping.yu@ieee.org

Extended author information available on the last page of the article

1 Introduction

With the advent of the era of big data, artificial intelligence is developing rapidly. At the same time, the in-depth research on artificial intelligence and deep learning has enabled related technologies to be applied to more fields, and applications in the financial services industry are becoming more and more popular[1–3]. On the other hand, with the integration of the rapidly developing multimedia devices and the financial industry, a large number of financial service images have sprung up. For users with constrained resources, especially for an extremely benefit-sensitive industry such as financial services, how to store these images related to financial services has become an urgent issue to be solved. Considering Storage as a Service (STaaS) presented by service provider companies like Amazon, Mosso, Sun, etc is one of the emerging services in cloud technology, it provides a massive and scalable storage capacity of the cloud[4, 5]. To take full advantage of the great convenience brought by the cloud environment, many studies have researched the storage of data in the cloud[6–15], which also include the outsourced storage of multimedia data. We mainly focus on financial services image storage outsourcing in this paper.

Outsourcing financial services images to the cloud will lose the ability to directly manage data for the local users. Popular social network providers commonly utilize image data to realize behavioral advertising, preference analytics, etc.[16]. Take Facebook and Flickr for example, for improved user experience in social discovery, they extract valuable features from user uploaded images without the knowledge of user and construct corresponding data mining models[17–19]. From this perspective, this caused information leakage and brought security risks. Notably, financial service images involve users' personal property information, and the problems caused by the leakage of sensitive information in such images cannot be ignored. The research of privacy-preserving image storage outsourcing is not new, so "Why do we study this problem again?" This is due to the rapid update of deep learning techniques, especially in the field of image processing, such as panoptic segmentation, object detection, object recognition, face recognition, fingerprint recognition provides technical support for the relevant departments. The organizations apply deep learning methods or models to extract information from massive images to get available models, such as face recognition systems. The service provider exposes the images from users to the organization for commercial benefits. Then the organization uses these images to train face recognition models. For individuals, their identities and other information are equivalent to publicity. If there are evildoers, they are likely to threaten their property and identity security. The artificial intelligence (AI) era has brought the secure issue of the image to a whole new level. In order to deal with the problems caused by these deep learning tools, it is urgent for us to propose corresponding deep learning approaches to efficiently process massive financial service images and protect privacy.

To prevent the servers or others from obtaining sensitive information from the financial service images that the client upload to do other illegal things. Inspired by the approach for text data storage proposed in[20], we considered extending the idea to multi-media data field. However, there are some difficulties: (1) There are many redundant information in the financial service image, and it is unreasonable to directly apply the encryption method for text; (2) The existing more popular image encryption algorithms only consider the encryption of the entire image[20–22], which causes a more expensive waste of computing resources; (3) There are also some schemes[12, 23] that introduce deep recognition methods and only process sensitive information. In these schemes, irreversible methods(blur, mosaic, pixilation, etc.) are directly applied to protect the privacy security, direct application of such methods due to different purposes will cause difficulties in the subsequent

acquisition and utilization of images. Therefore, we proposed a Web-based practical privacy-preserving distributed image storage for financial service system architecture in cloud computing. The architecture we proposed is designed to distribute financial service images with sensitive information to different cloud servers without causing big overhead and delay. Figure 1 illustrates this architecture of the system model we proposed.

The significance of the proposed architecture is that it can efficiently process a large number of financial service images and protect the privacy of clients. This approach is adaptable to different levels of security requirements for users. For the clients, it can solve the shortcomings of insufficient local storage capacity and protect privacy and security. For the servers, it can make full use of its resources to avoid resource waste. In this paper, our main contributions are as follows.

- We propose a novel lightweight privacy-preserving system architecture, which can solve the problem of secure outsourcing of a large number of financial service images.
- We put forward to apply deep networks EfficientDet for multi-class detection and classification of sensitive objects, completing the detection of sensitive objects and further realizing efficient financial service images classification.
- We propose a simple and reversible image encryption method to protect financial service images with sensitive information. Combined with chaotic map, the original image pixel value is converted to a pseudo-random number in the frequency domain that does not reveal the original information.
- Experimental results show that our proposed framework can more efficiently and more safely handle a large number of financial service image storage outsourcing comparing with these most popular image encryption algorithms.

This paper is organized as follows. In Section 2, we introduce the related works briefly. Then, we describe the proposed system architecture, security model, and design goals in Section 3. We present our scheme and experiment in Sections 4 and 5, respectively. Finally, we describe our conclusions and future research directions in Section 6.

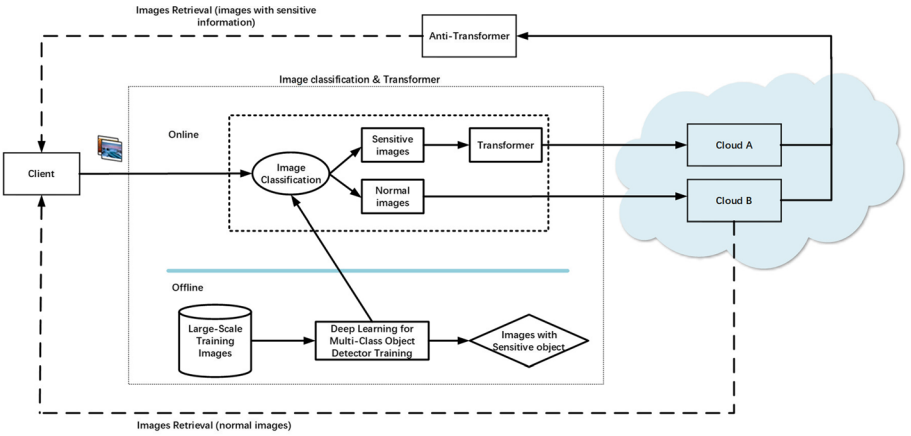

Fig. 1 System Architecture of Our Proposed Scheme

2 Related work

2.1 Security issues in cloud storage

Although cloud storage brings convenience to users, the security issues that follow it also hinder its development. There are a lot of security issues at the moment: 1)In the process of data transmission, the transmitted data may be attacked by malicious users; 2) On the server-side, the server itself is data abuse or attacked by malicious users for the benefit. In recent years, secure data storage has attracted a lot of attention[24–28]. A new remote data auditing method is proposed by Sookhak et al.[29], which realizes the protection of data storage in cloud computing based on algebraic signatures with less computational overhead, and solves the problem of data integrity verification in insecure and unreliable cloud servers. Kartit et al. proposes an architecture that can achieve encryption/decryption [30]. In this architecture, only authorized users can decrypt data when data is obtained from the cloud, thereby realizing data security issues. A new P2DS architecture is proposed in [31], which is a method of active defense, using attribute-based encryption and data self-determining mode to protect the private information of financial customers. Qiu et al.[32] proposes a method of using attribute-based access control and data word determinism to actively protect the private information of financial customers. This method can actively prevent the user's data from being affected by unexpected operations in the cloud, can deal with dynamic threats, and has a higher level of security sustainability. As an example to obtain secure real-time multimedia data sharing and transmission, a safe and effective data sharing and transmission model is proposed, which aims to protect cloud-based ITS implementation [33]. The shadow coding method is proposed to ensure the privacy in data transmission without affecting the recovery from multi-party data collection, to solve the distributed data sharing with privacy protection requirements [34]. For the storage of images, Zhang et al.[35] proposes a POP framework and a new non-interactive privacy protection protocol, which achieves the safe outsourcing of image storage and search. And the experiment proved that no additional communication and computing overhead was caused. Starting from the cloud, a picture encryption scheme that simultaneously realizes content-based picture retrieval is proposed[36]. Wang et al.[10] considers a cloud computing environment that requires secure watermark detection and privacy protection of multimedia data storage, and uses secure multi-party computing to propose an architecture based on compressed sensing. However, the main concern of the article is the security watermark detection to ensure that the uploaded pictures are copyright protected. Marwan et al.[11] proposes outsourcing storage for medical data and corresponding privacy protection methods for data protection to achieve safe medical image storage on the cloud. In [12], although an outsourced privacy protection image storage scheme is proposed, which encrypts image features through probabilistic encryption and deterministic encryption to achieve privacy protection, the main focus of this paper is on efficient privacy protection searchable technology. Vengadapurvaja et al. [13] proposes an approach which uses homomorphic encryption to protect the privacy of the medical images, and then outsources them to the cloud for storage. Although the above studies have studied the storage outsourcing of images to varying degrees, there are still very few related studies on massive images. Especially in the current era of artificial intelligence, from this perspective, this paper achieves the secure outsourcing of local image storage in the big data environment.

2.2 Distributed storage

The security of cloud computing has been extensively studied, and many cloud-based privacy protection methods have been proposed. Adopting several techniques to solve the security of data store in the multi-cloud architecture. The distributed storage based cloud can provide the huge number of services and maintain the data secure have been proved[37]. A technique to solve the security issues over data stored in the cloud is proposed called Secure-Split-Merge (SSM) Technique, this technique uses a unique mechanism of performing splitting of data using AES 128 bit encryption key and maintains these chunks of encrypted splits on different cloud server[38]. Olanrewaju et al. propose [39] a Reliable Framework for Data Administration (RFDA) using a split-merge policy using 128 AES encryption key to provide a secure authentication in the data sharing technique in the cloud is proposed. For secure distributed big data storage in cloud computing, Li et al. [40] proposes a framework and a simple data encryption approach. To protect the security of data in the cloud, a secure disintegration protocol (SDP) has been proposed in [41]. A novel framework is proposed by Zibouh et al.[42], which is based on various powerful security techniques such as secret sharing schema, Fully Homomorphic Encryption (FHE), and multi-cloud approach to achieve secure cloud computing. Subramanian et al.[43] used a new security model with an algorithm to reduce the threats caused by malicious insiders and malicious users and ensure the security of data sharing in the multi-cloud.

2.3 Object detection

In recent years, tremendous progress has been made in the field of object detection. State-of-the-art object detectors have emerged for more efficient detection. Existing object detectors are classified as two-stage [44–46]and one-stage [47–50] networks. The criteria depend on whether they have a region-of-interest proposal step or not. Compared with the flexibility and accuracy of the two-stage network, the one-stage network has attracted the attention of a large number of researchers due to its simpler and more efficient performance recently [51–53]. In particular, EfficientDet was proposed by [54], which consistently achieves better accuracy with much fewer parameters and FLOPs than previous object detectors. The experimental results confirm that the network can consistently achieve much better efficiency than prior art across a wide spectrum of resource constraints.

2.4 Chaotic map

Chaotic has excellent intrinsic properties of pseudo-randomness, ergodicity, and high sensitivity to initial conditions and parameters, since it is widely applied in image encryption[55]. To improve the complexity of the map and obtain better chaotic performance, researchers have proposed many chaotic maps from simple to complex. Existing chaotic maps are mostly categorized as one dimensional[55–57] and hyper-dimensional [20, 58–60] according to the dimension. Regardless, with the development of these studies, chaotic maps with better and better performance have been proposed recently [61, 62]. The pseudo-random numbers generated by these chaotic maps provide better basic conditions for the development of image encryption and other fields. In this paper, we mainly take 2D LSCM chaotic map[20] as an example.The 2D-LSCM is defined as:

$$\begin{cases} x_{i+1} = \sin\left(\pi\left(4\mu x_i\left(1-x_i\right)+(1-\mu)\sin\left(\pi y_i\right)\right)\right) \\ y_{i+1} = \sin\left(\pi\left(4\mu y_i\left(1-y_i\right)+(1-\mu)\sin\left(\pi x_{i+1}\right)\right)\right) \end{cases} \tag{1}$$

where μ is the control parameter and it has an interval of $[0, 1]$. The 2D-LSCM has chaotic behavior when $\mu \in (0,\ 1)$, and has hyperchaotic behavior when $\mu \in (0,\ 0.34) \cup (0.67,\ 1)$.

3 Problem formulation

3.1 System architecture

The system architecture we proposed in this paper is illustrated in Figure 1. Our system mainly involves two different parties: *Client* and *Cloud Servers*. Due to the inability to meet the required calculation requirements, the *Client* would like to outsource an expensive task to *Cloud Servers*, which possesses massive storage capacity and significant computational power. In our system, the *Client* classified a large number of pictures at local, and the results include images with sensitive information and normal images. Then for the sensitive images, apply the transformation algorithm we proposed to protect sensitive information from leaking and upload the two results to two different Cloud Servers. The details of the image classification and transformation algorithm are shown in Figure 1. For the normal images, upload directly them to *Cloud Servers*. The cloud server is mainly responsible for the storage task of a large number of images.

Client The *Client* is an entity that possesses many images but low storage capacity. Thus, to make full use of the storage capacity of the cloud server, the *Client* uses deep learning target detection methods to classify these large numbers of images, and then find sensitive images and execute the transformation algorithm we propose on these images to protect the privacy of the images. At last, upload the obtained results to two cloud servers respectively. For the normal images, upload directly them to *Cloud X* to cloud storage.

Cloud X Cloud X is a cloud server that possesses significant storage capacity to meet the storage requirements. This entity mainly stores the images obtained from the *Client*.

3.2 Security model

However, new challenges and threats to information assets residing in the cloud are introduced because the data stored remotely is out of users' control. We consider part of the image with sensitive information owned by the *Client* to be private. The goal of the *Client* is to enable *Cloud X* to store a large number of images while protecting the privacy of these images with possibly sensitive information. In our security model, the *Cloud X* is called the honest-but-curious and independent model. In other words, the *Cloud X* is assumed to faithfully follow the steps of the protocol, but it still tries to infer from or analyzes the data flow to learn sensitive information. In our design, the *Client* uploads his/her images with possibly sensitive information in a split form to two independent cloud entities, which store the results respectively. For those normal images, the *Client* directly uploads them to *Cloud X*. The assumption that cloud servers are mutually independent is promised by the independent reputation and financial interests of the cloud service provider. Here, *Cloud X* would explicitly state non-collusion in their legally binding documents. [63] confirmed that it can be achieved in practice to ensure the independence of cloud entities.

3.3 Design goals

Our ultimate goal is to design a practical and lightweight privacy protection image storage system that can outsource local image storage services while protecting client privacy security and maintaining efficiency. The goal is formally defined as a tuple (*ImgP*, *CompS*, *StorS*, *ClouE*) of four different design goals for cloud or client, where:

ImgP is a privacy protection algorithm that hides the original image plaintext information through encryption or privacy protection, and obtains ciphertext image information that is not related to the plaintext. As mentioned in previous section, the cloud entities should get no access to the possible privacy information of images. Images carry a lot of information, which may reveal sensitive information about the user (face, license plate, personal preferences, friends, family, etc.), and some do not provide personal information about the user, such as landscape, objects, animals, etc. For the necessity to protect the sensitive information I_{sen} in the image from leaking, we consider two solutions: 1) Only protect the sensitive information part of the image; 2) Protect the entire image. The latter on the one hand causes a large amount of encryption time consumption, on the other hand, a large amount of additional space consumption in distributed storage. In addition, the part carrying sensitive information may only occupy a small part for an image. Encrypting the entire image directly will inevitably cause a waste of resources. In order to protect privacy while not incurring large computation or storage costs, we finally determine to apply the former. Equation (2) describes the privacy protection process, where p_{ij} is the pixel value of the plaintext domain, and C_{ij} represents the ciphertext pixel.

$$C_{ij} \leftarrow ImgP\left(P_{ij}\right), \forall P_{ij} \in I_{sen} \tag{2}$$

CompS is a metric. The entire scheme can use the rich computing resources of the cloud to solve the problem of the lack of client resources compared with the traditional solution from the perspective of the client. The computing burden of the *Client* is mainly involved classifying sensitive images *CompC* and protecting the privacy of sensitive images *CompE*. It is undoubtedly an extremely time-consuming task that performing ordinary machine learning methods on a large number of images. Thus, we choose deep learning methods to classify images. It is a key step that the selection of encryption methods for privacy protection. In any case, the computing cost of the *Client* should be acceptable. This process is defined as:

$$Sum(CompC) + n * CompE_{new} < n * CompE_{original} \tag{3}$$

where n is the number of images need to outsource and the *Sum* function represents the total cost of classifying all images.

StorS is the local storage space. Obviously, we outsource a large amount of image storage tasks to the cloud, which greatly saves local storage space. It is defined by:

$$StorS_o(client) < StorS_b(client) \tag{4}$$

ClouE It should be efficient to obtain and use encrypted images which have been outsourced to the cloud. Our system should be simple about obtaining these images, which

means that the privacy protection methods are reversible and efficient. The (5) represents the decryption process $re - ImgP$ of the image encryption algorithm.

$$P_{ij} \leftarrow re - ImgP\left(C_{ij}\right), \forall P_{ij} \in I_{sen} \tag{5}$$

4 The design of our proposed system

The system we proposed mainly contains two components: 1) a sensitive information detection process(SIDP); 2) an image distributed Storage Process(IDSP). The purpose of the former is to determine whether the input image requires a higher level of security guarantee. The latter is designed to protect sensitive information from adversaries. A more detailed description of the design of these two components is as follows:

4.1 Sensitive information detection process

The SIDP determines whether the image needs to be distributed and stored on different cloud servers. The IDSP will be applied to images that carry sensitive information. The sensitive information in the image refers to the part of the information related to the personal identifier that is directly or indirectly leaked, such as: face, fingerprint, license plate, family, friends, etc. The disclosure of this information may bring reputation and property security issues to individuals. For images that carry such information, we call them sensitive images. Our system model only performs conversion operations. The following provides detailed explanations about the process of performing sensitive information detection.

Setup The security level of the input image is an alternative, and the security level can be determined by the named label. The image owners or cloud service provider configures a label pool to achieve higher security requirements. Based on the labeled pool, the training images are labeled and used as the input of the deep neural network to train the neural network. This paper takes human faces and license plates as examples.

Sensitive Information Detection Adopt the above trained neural network to detect input images, separate images carrying sensitive information, and mark the location of sensitive information.

Output In our model, two types of images are output. The one type is a normal image, which is uploaded directly to the cloud server. The other is an image with sensitive information. The following Transformation operations need to be performed to prevent information leakage.

The purpose of performing the Sensitive information detection process(SIDP) in the proposed model is to reduce the cost of computing resources and computing burden by image classification task. In order to meet the needs of lightweight and ensure accuracy, we adopt the EfficientDet as the detection network here. Notably, our target detection network is based on EfficientDet and might not be optimal, but this method is more suitable than other methods in resource-saving. Without loss of generality, training of our model is conducted jointly on WIDER FACE[64] and CCPD2019[65]. The target detection network is trained to handle the detection of face and license plate simultaneously. Notely, the selection of the detection network and the setting of

sensitive information are flexible and adjustable. For example, in some scenarios, such as medical, financial, or transportation industries, we can set the corresponding security level, select the corresponding data set, and jointly train the network model to improve the flexibility and wide applicability of the network for meeting the needs of different industries.

4.2 Image distributed storage process

In this section, there are mainly two algorithms to support our security model, including efficient image distributed storage algorithms and efficient image merging algorithms. Finally achieving the privacy protection of images through these algorithms.

1) *Secure Efficient Image Distributions Storage algorithm*

The Secure Efficient Image Distributions Storage(SEIDS) algorithm is designed to realize image processing before uploading to the cloud. The algorithm is the details of Transformation in Figure 1. The image carrying sensitive information and random parameters as the input. The input is two separated encrypted images. We achieve the transformation of image from the numerical domain to the phase domain before sending them to the cloud by this process. So as to prevent privacy leakage and realize image privacy protection.

Assuming that the image is represented as A, the pixel value in A is a. The element in the random matrix generated by the 2D LSCM chaotic map is represented as b. In order to perform the transformation process, we first apply the chaotic map to generate a 2D random matrix, where b is in the interval of $[0, 255]$. If necessary, you can refer to [20] for more usage details of 2D LSCM chaotic map. Based on the tangent and arctangent functions, the numerical value can be converted into the phase domain through the (8). Notely, we need to ensure that the denominator a is not equal to zero in fractions. For this reason, during the transformation process, we initialize a buffer to store the pixels of the original image with the pixel value of 0. In addition, if b is 0, $b \backslash a$ is 0 regardless of the value of a. To solve this problem, we fine-tune the range of values generated by the chaotic map and use (9) to complete the transformation process. As shown in the (7), the value of the generated random number is between 1 and 255.

$$b' = \mathrm{mod}\left(\left\lfloor b \times 10^{16} \right\rfloor, 256\right) \tag{6}$$

$$b' = \mathrm{mod}\left(\left\lfloor b \times 10^{16} \right\rfloor, 255\right) + 1 \tag{7}$$

$$c = \mathrm{mod}\left(\arctan\left(\frac{b'}{a}\right), 256\right) \tag{8}$$

$$\begin{cases} c = \mathrm{mod}\left(\arctan\left(\frac{b'}{a}\right), 256\right), a \neq 0 \\ c = \mathrm{mod}\left(\arctan\left(b'\right), 256\right), a = 0 \end{cases} \tag{9}$$

Then, in order to hide the angle information obtained above, we select other parameters to generate a new chaotic matrix K by (1) and (7). For each $k \in K$, add it to the value obtained from the (9). It can be described as following:

$$\begin{cases} c = \mathrm{mod}\left(\left(\arctan\left(\frac{b'}{a}\right) + k\right), 256\right), a \neq 0 \\ c = \mathrm{mod}\left(\left(\arctan\left(b'\right) + k\right), 256\right), a = 0 \end{cases} \tag{10}$$

Finally, outsource the segmented images C and K to different cloud, respectively.

Input: The original image A with sensitive information obtained from **Section 3**, Key for generating the pseudo-random number matrics
Output: Separated images C and D

for all $x \epsilon A$ **do**
  for all $y \epsilon A$ **do**
    if $A[x][y] \neq 0$ **then**
      $C[x][y] \leftarrow \left[\arctan\left(\frac{B[x][y]}{A[x][y]}\right) + K[x][y]\right] \bmod 256$
      // K and B generated by a $2D$ chaotic map by Key
    else
      put the (x, y) into a buffer pool $Buffer1$
      $C[x][y] \leftarrow [\arctan(B[x][y]) + K[x][y]] \bmod 256$
    end if
  end for
end for
$D \leftarrow B$ **return** C, D

The main steps of Algorithm 1 are explained as follows:

- Input parameters, use 2D LSCM chaotic mapping to generate pseudo-random number matrices B and K, with dimensions equal to the original picture A
- Based on the pseudo-random matrix generated in the previous step, encryption image C generated by $\left[\arctan(B/A) + K\right] \bmod 256$
- Upload two separate results: B and C to two different cloud servers

The implementation of secure efficient image distributed storage algorithms can prevent information leakage and meet the needs of privacy protection. Untrusted cloud server providers use the acquired user information including appearance, preference, property, and identity, etc. to extract data characteristics, build models to improve user experience or intentionally or unintentionally exposed the obtained user information to some unauthorized users for getting a certain benefit. It is assumed that the cloud server or a malicious user has access to the data on the server and possesses the key. For the cloud, the conditions for obtaining image information from the data are not enough, because the data obtained by the cloud server is partial. Another part of the data is stored elsewhere and cannot be accessed by a cloud server. Partial data do not contain any information since the original image will not be obtained until two parts are operated together. Some malicious users who want to abuse these images for illegal use, also face the same problems as the above model. Since the malicious user only accessed part of the information from the server, he would not obtain any sensitive information about the original image. Last but not least, the security of the pseudo-random matrix depends on the chaotic map used, and its security has been confirmed in[20]. In addition, the key of the encryption algorithm is composed of two chaotic map parameters, which enhances the anti-attack of the algorithm in some extent. Therefore, our proposed algorithm can effectively resist attacks from malicious users or cloud servers in theory. **Algorithm 1** shows the pseudo-code of the *SEIDS* algorithm.

2) *Efficient Image Merging algorithm*

The Efficient Image Merging algorithm(*EIM*) algorithm is designed to obtain original image information by the inverse transformation of two image components from two distributed cloud servers. The corresponding stage shown in Figure 1 is the anti-transformation. The input of the algorithm includes data components and parameters from two cloud servers. The output is the original images of the user. **Algorithm 2** shows the pseudo-code of *EIM*.

Input: Separated images C and D from two different cloud servers, the Key for chaotic map
Output: The original sensitive part A

```
Generate the corresponding pseudo-random number matrics by Key
for all x∈A do
    for all y∈A do
        if (x, y) ∈Buffer1 then
            A[x][y] = 0
        else
            temp ← tan(C[x][y] − K[x][y]) mod 256
            C[x][y] ← [arctan(B[x][y]) + K[x][y]] mod 256
            A[x][y] ← D[x][y]/temp
        end if
    end for
end forreturn A
```

The main stages of Algorithm 2 are given as follows:

- Input parameters, use 2D chaotic mapping to generate pseudo-random number matrices *B* and *K*, with dimensions equal to the original picture *A*
- Based on the pseudo-random matrix generated in the previous step, get the encryption image *C* and *D* from two clouds and then compute the original *A* by $D/(\tan(C-K) \bmod 256.)$
- Output the original image *A*

Using this method, the original image carrying sensitive information can be completely divided into two parts, and any private information about the original image will not be obtained from the cloud server of either party. From the perspective of an attacker or malicious user, it is almost impossible to obtain all the image parts and key information. Even if the adversary has access to the data, he will not obtain sensitive information. Besides, this scheme can effectively protect the user's sensitive information carried by images since the key value is randomly generated and any separated data does not carry any content information.

5 Experiment

To illustrate the problem of privacy protection image storage, this article implements our experiment with two privacy settings categories of the human face and license plate as examples. Considering the excellent performance of the network model in terms of efficiency and size, we finally selected the EfficientDet D0 as the detection network. In the

training phase, we directly finetune and make full use of a trained efficientdet d0 model based on the idea of using transfer learning. Our training is conducted jointly WIDER FACE and CCPD. Specifically, we arbitrarily select more than 6000 images from WIDER and select 10000 from the open data set to form a new dataset. Based on the newly formed dataset, we perform the training process. Thinking of the used dataset, we adjusted the input image size with 1024*1024 and some hyperparameters including the learning rate and others remain unchanged. Finally, we choose from the remaining dataset, more than 2000 images from WIDER FACE and more than 3000 images from CCPD, following the ratio of 1:3. We evaluate our model on this dataset with 5000s training images, achieving 73.8 AP for the detection of license plate and 29.5 AP for the detection of face. For the stage of training the model, considering the resources and efficiency, we can choose to complete it on the cloud server, which has nothing to do with our subsequent experimental evaluation. For the images that need to be outsourced, we first use the above-obtained model locally to identify sensitive information and then use the encryption method we propose to protect the sensitive information. Figures 2 and 3 illustrates the result of detection and encryption, respectively.

To protect the security of image data and prevent the impact of information leakage on users, we evaluate the privacy protection methods we proposed in this section. The experiment focuses on the efficiency of the encryption method (in the perspective of the execution time) and makes a comparison with the current popular image encryption methods.

Our experiment designed from two aspects: 1) evaluating whether different image encryption algorithm was impacted on the execution time; 2) the encryption time spent on different numbers of images between different image encryption, which was considered an important aspect in the current multimedia age. To make the experiment more convincing, we have carried out experiments using the same environments. We implement our experiment on python3.7, on Intel(R) Core(TM) i5-8265U CPU at 1.60GHz with 8GB of RAM running Window10.

5.1 Execution time comparison

For keeping fair, we tested 20 social images for different sizes of images($256 * 256$, $512 * 512$, and $1024 * 1024$), and averaged them as the execution time. Table 1 conducts experiments on the encryption time required for images of different sizes, and compares them with three popular image encryption algorithms. To ensure that the results are reasonable and convincing, we reproduced the other three algorithms using the same python language as our algorithm. It can be seen from the results that no matter which algorithm, the time required increases as the image size increases. Our proposed scheme takes almost the same time as Fast_en[21] and is lower than the encryption schemes proposed by LSCM_en[20] and CTBCS_en[22].

Figure 4 shows the comparison result of the size of encrypted data. We only considered the time spent by the encryption algorithm itself, that is to say, at this stage, to compare the efficiency of the encryption algorithm, we discarded the sensitive object recognition stage and encrypt the entire image. It can be seen that our approach is the most time-saving. Under the condition of different sizes of images, the time taken by other algorithm is about 2 to 5 times that of our proposed. The results also show our encryption algorithm in this scheme is more efficient with the comparison of other image encryption algorithms.

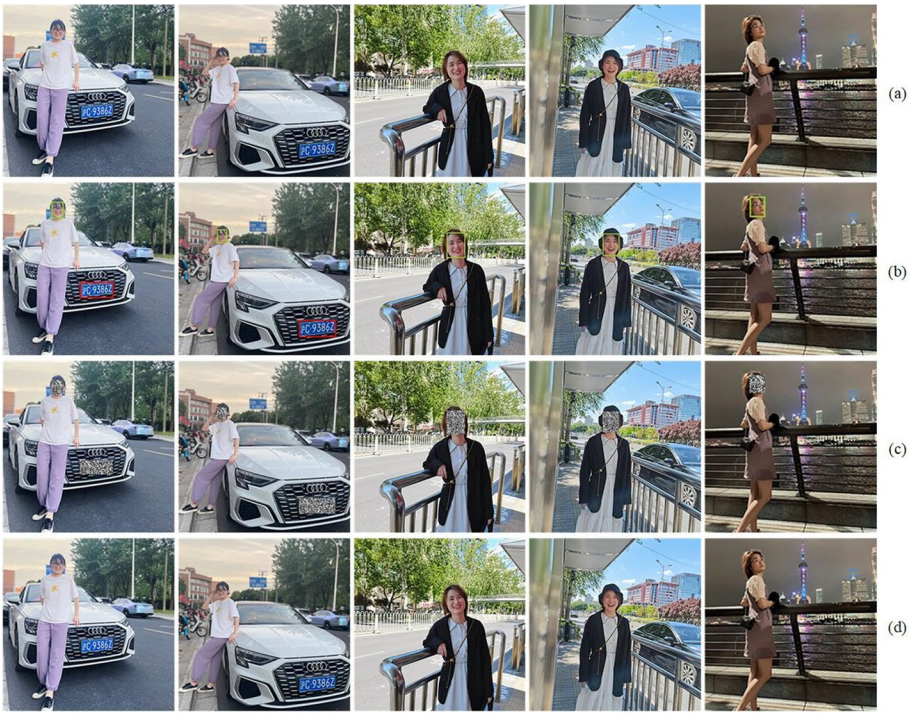

Fig. 2 Our experimental results on the social images by the proposed system architecture: (a)the orignal images; (b) the detection results of SIDP; (c) the encrypted images of the transformation process; (d) the decrypted images

5.2 Performance comparison

In evaluating the execution time on different numbers of images with different image encryption, the experimental deployment settings with the different number of images from social network are as follows: 1,10,20,30,40,50,60,70,80,90,100.

The Table 2 describes the results of different numbers of images under different encryption schemes compared with our proposed lightweight privacy-preserving scheme. The test images are from the WIDER FACE dataset. In order to ensure the rationality and convincing of the experiment, we do 20 experiments for each group of experimental results, and then calculate the average value as the final result. We test against 10 images, and then calculate the time spent encrypting a single image to obtain the first row in the table. For our scheme, it is mainly composed of two parts: the time spent classifying sensitive part of images *CompC* and the time spent protecting the privacy of sensitive part of images *CompE*. The time required to identify sensitive information depends on the deep model we use, and the length of encryption depends on the size of the sensitive area and the number of images. For the other three schemes, the time spent depends on the image size and number of images. From the results in the Table 2, it can be seen that the time required for the two parts of our scheme is mainly *CompC*. Considering that only the sensitive part needs to be encrypted, so the encryption time is much lower than the other three schemes. Our scheme is lower than the other three schemes related to the total time spent. And as the

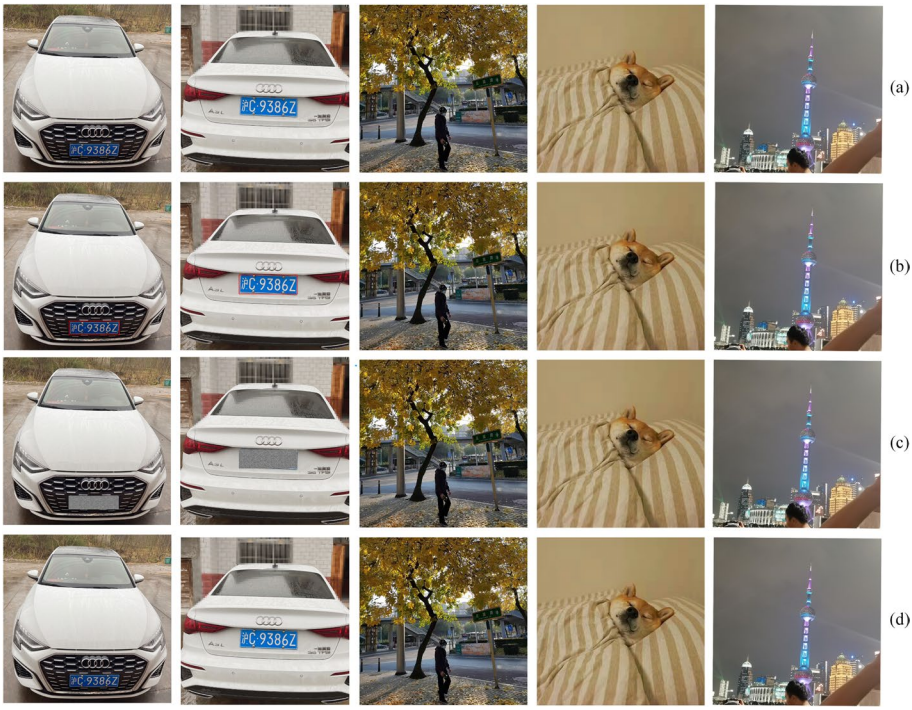

Fig. 3 Our experimental results on the social images with sensitive or normal information by the proposed system architecture: (a)the orignal images; (b) the detection results of SIDP; (c) the encrypted images of the transformation process; (d) the decrypted images

Table 1 Encryption time (second) of different image encryption algorithms for images with different sizes

Image size	Our proposed	LSCM_en[20]	Fast_en[21]	CTBCS_en[22]
256	0.64858	1.18427	0.64387	0.98802
512	2.55336	4.73764	2.61018	4.07901
1024	10.43923	18.42175	10.76967	16.68141

number of images increases, this gap is getting bigger and bigger. Therefore, our scheme exhibits more superior performance as the number of images increases.

Figure 5 shows the comparison of execution time under the different number of images. It can be seen that our scheme costs less time than Fast_en[21],CTBCS_en[22]and LSCM_en[20]. As the number of images increases, the execution time of any schemes is increasing. However, as can be seen from Figure 5, the growth rate of our program is more gradual. This feature makes our proposed scheme perform better in transmitting a large number of images.

The privacy protection image model we proposed has better efficiency. Due to the encryption algorithm we proposed transforms the sensitive information from the numerical domain to the phase domain, intuitively, it completely changes the original information; In addition, because of our proposed cloud-based distributed storage architecture, for a single

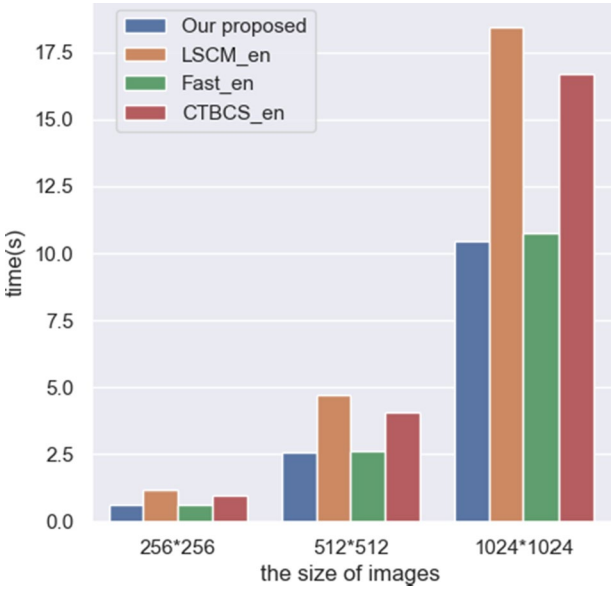

Fig. 4 The comparison of the time required for different size of images with different algorithm

cloud server, only part of the information of the picture is stored. Therefore, neither the adversary nor the malicious server can obtain the sensitive information in the picture. From the above comparative experiments, we can see that the privacy protection algorithm proposed in the article is more efficient, especially under a large number of images, the proposed scheme can show higher efficiency. All in all, our proposed architecture shows better performance in terms of efficiency and privacy protection.

6 Conclusion

In this paper, we propose a Web-based privacy-preserving financial service image storage architecture in cloud computing, which realizes the outsourcing of financial service multimedia image storage tasks, prevents the sensitive information leakage of users and protects the privacy of users. In the storage of multimedia data related to financial service, the architecture has strong flexibility and universal applicability. In other words, we can select the corresponding neural network model and sensitive information settings according to

Table 2 Performance (second) comparison of different numbers of images under different encryption schemes

Number of images	Our proposed			LSCM_en[20]	Fast_en[21]	CTBCS_en[22]
	CompC	*CompE*	*CompC* + *CompE*			
1	1.00265	0.23235	1.23500	2.32739	1.37033	1.82657
10	10.03184	2.76296	12.7948	26.78278	15.79953	23.85293
100	87.42914	25.74682	113.17596	266.06007	163.97846	221.26220
1000	1007.95034	229.46078	1237.41112	3070.23437	1611.74418	2118.20771

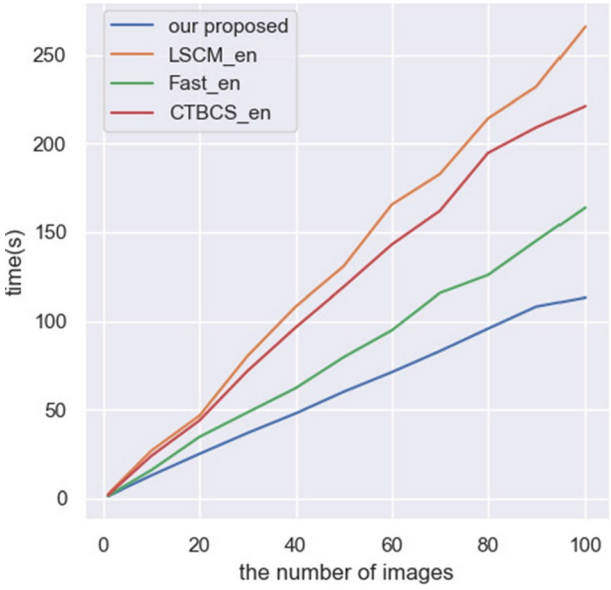

Fig. 5 The comparison of the time required for different numbers of images with different algorithm

the needs. Based on the comparison of the current popular image encryption algorithms, the privacy protection scheme we proposed shows better efficiency in outsourcing the privacy protection of a large number of financial service images. However, there are still some shortcomings. For example, in the outsourcing of financial service image storage, distributed storage, although protecting privacy and security, produces additional information, which causes a certain amount of storage space loss for the cloud. This is also an aspect that we will focus on in the future.

Declarations

Conflicts of interest The authors declare that they have no conflict of interest.

References

1. Board, F.S.: Artificial intelligence and machine learning in financial services: Market developments and financial stability implications. Financial Stability Board 45 (2017)
2. Tan, L., Yu, K., Ming, F., Cheng, X., Srivastava, G.: Secure and resilient artificial intelligence of things: A honeynet approach for threat detection and situational awareness. IEEE Consum. Electron. Mag. **11**(3), 69–78 (2022). https://doi.org/10.1109/MCE.2021.3081874
3. Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A.K., Khan, F.A.: Securing critical infrastructures: Deep-learning-based threat detection in iiot. IEEE Commun. Mag. **59**(10), 76–82 (2021). https://doi.org/10.1109/MCOM.101.2001126
4. Bagaeen, A., Al-Zoubi, S., Al-Sayyed, R., Rodan, A.: Storage as a service (staas) security challenges and solutions in cloud computing environment: An evaluation review. In: 2019 Sixth HCT Information Technology Trends (ITT), pp. 208–213. IEEE (2019)
5. Marinescu, D.C.: Cloud Computing: Theory and Practice. Morgan Kaufmann, (2017)
6. Mason, R.S., Rodriguez, A.: Method and system for interfacing to cloud storage. Google Patents. US Patent 8,880,474 (2014)

7. Chacko, P.: Distributed virtual storage cloud architecture and a method thereof. Google Patents. US Patent 9,128,626 (2015)
8. Obrutsky, S.: Cloud storage: Advantages, disadvantages and enterprise solutions for business. In: Proceedings of the Eastern Institute of Technology Conference, p. 10 (2016)
9. Yu, J., Ren, K., Wang, C.: Enabling cloud storage auditing with verifiable outsourcing of key updates. IEEE Trans. Inf. Forensics Secur. **11**(6), 1362–1375 (2016)
10. Wang, Q., Zeng, W., Tian, J.: A compressive sensing based secure watermark detection and privacy preserving storage framework. IEEE Trans. Image Process. **23**(3), 1317–1328 (2014)
11. Marwan, M., Kartit, A., Ouahmane, H.: A framework to secure medical image storage in cloud computing environment. J. Electron. Commer. Organ. (JECO) **16**(1), 1–16 (2018)
12. Ferreira, B., Rodrigues, J., Leitao, J., Domingos, H.: Practical privacy-preserving content-based retrieval in cloud image repositories. IEEE Trans. Cloud Comput. **7**(3), 784–798 (2017)
13. Vengadapurvaja, A., Nisha, G., Aarthy, R., Sasikaladevi, N.: An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia Comput. Sci. **115**, 643–650 (2017)
14. Feng, C., Yu, K., Aloqaily, M., Alazab, M., Lv, Z., Mumtaz, S.: Attribute-based encryption with parallel outsourced decryption for edge intelligent iov. IEEE Trans. Veh. Technol. **69**(11), 13784–13795 (2020)
15. Yang, L., Yu, K., Yang, S.X., Chakraborty, C., Lu, Y., Guo, T.: An intelligent trust cloud management method for secure clustering in 5g enabled internet of medical things. IEEE Transactions on Industrial Informatics, 1–1 (2021). https://doi.org/10.1109/TII.2021.3128954
16. Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., Cranor, L.: Why johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 589–598 (2012)
17. Malheiros, M., Jennett, C., Patel, S., Brostoff, S., Sasse, M.A.: Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 579–588 (2012)
18. Zhang, Y., Ma, X., Zhang, J., Hossain, M.S., Muhammad, G., Amin, S.U.: Edge intelligence in the cognitive internet of things: Improving sensitivity and interactivity. IEEE Network **33**(3), 58–64 (2019)
19. Lu, H., Zhang, Y., Li, Y., Jiang, C., Abbas, H.: User-oriented virtual mobile network resource management for vehicle communications. IEEE transactions on intelligent transportation systems (2020)
20. Hua, Z., Jin, F., Xu, B., Huang, H.: 2d logistic-sine-coupling map for image encryption. Signal Process. **149**, 148–161 (2018)
21. Wang, X., Feng, L., Zhao, H.: Fast image encryption algorithm based on parallel computing system. Inf. Sci. **486**, 340–358 (2019)
22. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**, 403–419 (2019)
23. Yu, J., Zhang, B., Kuang, Z., Lin, D., Fan, J.: iprivacy: Image privacy protection by identifying sensitive objects via deep multi-task learning. IEEE Trans. Inf. Forensics Secur. **12**(5), 1005–1016 (2017). https://doi.org/10.1109/TIFS.2016.2636090
24. Sun, Y., Liu, J., Yu, K., Alazab, M., Lin, K.: Pmrss: Privacy-preserving medical record searching scheme for intelligent diagnosis in iot healthcare. IEEE Trans. Industr. Inform. (2021)
25. Sun, Y., Cui, Y., Huang, Y., Lin, Z.: Sdmp: A secure detector for epidemic disease file based on dnn. Inf. Fusion **68**, 1–7 (2021)
26. Tan, L., Yu, K., Shi, N., Yang, C., Wei, W., Lu, H.: Towards secure and privacy-preserving data sharing for covid-19 medical records: A blockchain-empowered approach. IEEE Trans. Netw. Sci. Eng. (2021)
27. Han, H., Fang, L., Lu, W., Zhai, W., Li, Y., Zhao, J.: A gcica grant-free random access scheme for m2m communications in crowded massive mimo systems. IEEE Internet Things J. **9**(8), 6032–6046 (2022). https://doi.org/10.1109/JIOT.2021.3110793
28. Xu, D., Yu, K., Ritcey, J.A.: Cross-layer device authentication with quantum encryption for 5g enabled iiot in industry 4.0. IEEE Trans. Industr. Inform, 1–1 (2021). https://doi.org/10.1109/TII.2021.3130163
29. Sookhak, M.: Dynamic remote data auditing for securing big data storage in cloud computing. PhD thesis, University of Malaya (2015)
30. Kartit, Z., El Marraki, M.: Applying encryption algorithm to enhance data security in cloud storage. Eng Lett 23(4) (2015)
31. Gai, K., Qiu, M., Thuraisingham, B., Tao, L.: Proactive attribute-based secure data schema for mobile cloud in financial industry. In: 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, pp. 1332–1337. IEEE (2015)

32. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H.: Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Gener. Comput. Syst. **80**, 421–429 (2018)
33. Gai, K., Qiu, L., Chen, M., Zhao, H., Qiu, M.: Sa-east: security-aware efficient data transmission for its in mobile heterogeneous cloud computing. ACM Trans. Embed. Comput. Syst. (TECS) **16**(2), 1–22 (2017)
34. Liu, S., Qu, Q., Chen, L., Ni, L.M.: Smc: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Trans. Big Data **1**(2), 68–81 (2015)
35. Zhang, L., Jung, T., Liu, C., Ding, X., Li, X.-Y., Liu, Y.: Pop: Privacy-preserving outsourced photo sharing and searching for mobile devices. In: 2015 IEEE 35th International Conference on Distributed Computing Systems, pp. 308–317. IEEE (2015)
36. Ferreira, B., Rodrigues, J., Leitao, J., Domingos, H.: Privacy-preserving content-based image retrieval in the cloud. In: 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), pp. 11–20. IEEE (2015)
37. Bohli, J.-M., Gruschka, N., Jensen, M., Iacono, L.L., Marnau, N.: Security and privacy-enhancing multicloud architectures. IEEE Trans Dependable Secure Comput **10**(4), 212–224 (2013)
38. Khan, B.U.I., Baba, A.M., Olanrewaju, R.F., Lone, S.A., Zulkurnain, N.F.: Ssm: Secure-split-merge data distribution in cloud infrastructure. In: 2015 IEEE Conference on Open Systems (ICOS), pp. 40–45. IEEE (2015)
39. Olanrewaju, R.F., Khan, B.U.I., Baba, A., Mir, R.N., Lone, S.A.: Rfda: Reliable framework for data administration based on split-merge policy. In: 2016 SAI Computing Conference (SAI), pp. 545–552. IEEE (2016)
40. Li, Y., Gai, K., Qiu, L., Qiu, M., Zhao, H.: Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf Sci **387**, 103–115 (2017)
41. Rawal, B.S., Vijayakumar, V., Manogaran, G., Varatharajan, R., Chilamkurti, N.: Secure disintegration protocol for privacy preserving cloud storage. Wirel. Pers. Commun **103**(2), 1161–1177 (2018)
42. Zibouh, O., Dalli, A., Drissi, H.: Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach. J. Theor. Appl. Inf. Technol. **87**(2), 300 (2016)
43. Subramanian, K., John, F.L.: Secure and reliable unstructured data sharing in multi-cloud storage using the hybrid crypto system. IJCSNS **17**(6), 196–206 (2017)
44. Ren, S., He, K., Girshick, R., Sun, J.: Faster r-cnn: Towards real-time object detection with region proposal networks. arXiv preprint arXiv:1506.01497 (2015)
45. He, K., Gkioxari, G., Dollár, P., Girshick, R.: Mask r-cnn. In: Proceedings of the IEEE International Conference on Computer Vision, pp. 2961–2969 (2017)
46. Lin, T.-Y., Dollár, P., Girshick, R., He, K., Hariharan, B., Belongie, S.: Feature pyramid networks for object detection. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2117–2125 (2017)
47. Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.-Y., Berg, A.C.: Ssd: Single shot multibox detector. In: European Conference on Computer Vision, pp. 21–37. Springer (2016)
48. Sermanet, P., Eigen, D., Zhang, X., Mathieu, M., Fergus, R., LeCun, Y.: Overfeat: Integrated recognition, localization and detection using convolutional networks. arXiv preprint arXiv:1312.6229 (2013)
49. Redmon, J., Farhadi, A.: Yolo9000: better, faster, stronger. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 7263–7271 (2017)
50. Lin, T.-Y., Goyal, P., Girshick, R., He, K., Dollár, P.: Focal loss for dense object detection. In: Proceedings of the IEEE International Conference on Computer Vision, pp. 2980–2988 (2017)
51. Law, H., Deng, J.: Cornernet: Detecting objects as paired keypoints. In: Proceedings of the European Conference on Computer Vision (ECCV), pp. 734–750 (2018)
52. Zhao, Q., Sheng, T., Wang, Y., Tang, Z., Chen, Y., Cai, L., Ling, H.: M2det: A single-shot object detector based on multi-level feature pyramid network. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 9259–9266 (2019)
53. Zhou, X., Wang, D., Krähenbühl, P.: Objects as points. arXiv preprint arXiv:1904.07850 (2019)
54. Tan, M., Pang, R., Le, Q.V.: Efficientdet: Scalable and efficient object detection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 10781–10790 (2020)
55. Habutsu, T., Nishio, Y., Sasase, I., Mori, S.: A secret key cryptosystem by iterating a chaotic map. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 127–140. Springer (1991)
56. Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. Signal Process **138**, 129–137 (2017)

57. Kulsoom, A., Xiao, D., Abbas, S.A., et al.: An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and dna complementary rules. Multimed. Tools. Appl. **75**(1), 1–23 (2016)
58. Liu, W., Sun, K., Zhu, C.: A fast image encryption algorithm based on chaotic map. Opt. Lasers Eng. **84**, 26–36 (2016)
59. Kanso, A., Ghebleh, M.: A novel image encryption algorithm based on a 3d chaotic map. Commun. Nonlinear Sci. Numer. Simul. **17**(7), 2943–2959 (2012)
60. Hua, Z., Zhou, Y., Pun, C.-M., Chen, C.P.: Image encryption using 2d logistic-sine chaotic map. In: 2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 3229–3234. IEEE (2014)
61. Joshi, A.B., Kumar, D., Gaffar, A., Mishra, D.: Triple color image encryption based on 2d multiple parameter fractional discrete fourier transform and 3d arnold transform. Opt. Lasers Eng. **133**, 106139 (2020)
62. Luo, Y., Yu, J., Lai, W., Liu, L.: A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimed. Tools. Appl. **78**(15), 22023–22043 (2019)
63. Chen, R., Akkus, I.E., Francis, P.: Splitx: High-performance private analytics. ACM SIGCOMM Comput. Commun. Rev. **43**(4), 315–326 (2013)
64. Yang, S., Luo, P., Loy, C.-C., Tang, X.: Wider face: A face detection benchmark. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 5525–5533 (2016)
65. Xu, Z., Yang, W., Meng, A., Lu, N., Huang, H., Ying, C., Huang, L.: Towards end-to-end license plate detection and recognition: A large dataset and baseline. In: Proceedings of the European Conference on Computer Vision (ECCV), pp. 255–271 (2018)

Authors and Affiliations

Cai Xiaohong[1] · Sun Yi[1] · Lin Zhaowen[1] · Muhammad Imran[2] · Yu Keping[3,4]

Cai Xiaohong
cxh@bupt.edu.cn

Lin Zhaowen
Linzw@bupt.edu.cn

Muhammad Imran
dr.m.imran@ieee.org

[1] School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, NO 10 Xitucheng Road, Haidian District, 100876 Beijing, Beijing, China

[2] College of Applied Computer Science, King Saud University, 11692 Riyadh, Saudi Arabia

[3] Graduate School of Science and Engineering, Hosei University, Tokyo 184-8584, Japan

[4] RIKEN Center for Advanced Intelligence Project, RIKEN, Tokyo 103-0027, Japan