Access control mechanism based on image recognition and user level

Haojin Qi¹, Yong Wang¹, Yueping Yang¹, Xiaodie Yu² and Xiaoming Ju*²

¹ Ningbo Power Supply Company Information Communication Branch, State Grid Corporation of China, Zhejiang, 315000, China
² School Computer Science and Software Engineering, East China Normal University, Shanghai, 200062, China

*Corresponding author's e-mail: xmju@sei.ecnu.edu.cn

Abstract. The rapid development of big data and the Internet has brought enormous challenges to data security. Aiming at protecting the sensitive image data protection and secure access of information, an access control mechanism based on image recognition and user level is proposed. On the one hand, the mechanism is based on deep learning, mining sensitive information in images, realizing hierarchical classification and precise positioning of sensitive areas in images; on the other hand, combining identity authentication to achieve user management based on identity level; The image sensitivity level is mapped with the user identity level, which realizes the user's access authority control, prevents unauthorized or illegal access of sensitive image information, and effectively protects sensitive image information.

1. Introduction

Sensitive information mainly refers to data information that would cause serious damage to national interests, business operations, and data owners if leaked, falsified, stolen, misused, or not allowed to be transmitted [1]. With the rapid development of the Internet and big data, data sharing has become an indispensable part. In the process of data interaction, if there is no effective management and protection measures, it will cause leakage of sensitive information, which will have a negative impact. Therefore, access control mechanisms are needed to ensure the security and privacy of sensitive information.

In 2016, Chi[2] proposed the assertion attribute authentication based on user level, which binds user level and authority to enable users to access data resources within the scope of user level authority. The access subject and object are classified into domains and the fine-grained access control is realized. Shao[3] et al. proposed an attribute-based layered key exchange protocol in 2018. Data owners and visitors establish layered keys, and users decrypt and access data contents in accordance with security levels.

Current access control often focuses on the user level and is limited to the authorization protection of data [4], which grants or restricts users' rights to access data based on different standards. However, compared with encryption and permissions, it is important to accurately identify, discover and master the location of sensitive data. Moreover, data carriers are generally text, image, video, etc. Text can be filtered and recognized by setting sensitive words or themes [5], while sensitive images are seldom used in access control due to the complexity of content and different from general face recognition or...
image classification. In addition, a single image is often operated as a whole, but there are also sensitive and non-sensitive areas in the image, which are managed without distinction, resulting in the waste of resources. Therefore, the paper proposes an access control mechanism based on image recognition and user identity.

The main contributions are:

1) Partitioning individual image information based on sensitivity, rather than taking the whole image as an object, realizes the hierarchical and regional management of an image;
2) Image sensitivity level is defined. Based on Mobilenet_ssd model, sensitive areas in images are mined to realize recognition of sensitive areas and target positioning.
3) Combined with security assertion markup language (SAML) technology, user identity level is taken as target attribute to achieve hierarchical management of users; Combining the sensitivity level of image information with the user's identity level, a binary tree access mechanism is proposed to better manage and control sensitive areas and effectively protect sensitive information in images.

2. Related information

2.1. Mobilenet model
The Mobilenet network is a streamlined lightweight convolutional network proposed by Lecun Y et al. [6], and is currently mainly used for tasks such as image classification and detection. Its network architecture is shown in Figure 1. The biggest improvement between this network and the traditional network is that the standard convolution is decomposed into a 3*3 depthwise convolution and a 1*1 pointwise convolution [7].

![Figure 1. Mobilenet’s network architecture](image)

The advantage is that the calculation amount and network parameters of the model are greatly reduced, thereby improving the calculation efficiency of the model and speeding up the operation speed of tasks such as image classification and detection.

2.2. SSD model
The SSD model [8] is a regression detection-based target detection model proposed by LIU W et al. in 2016. The network architecture of the SSD model is shown in Figure 2. The input image size is 300*300. The backbone network of the model is a deep convolutional neural network (VGG-16 model), which realizes preliminary feature extraction of the target region in the image [9]; The convolution layer with decreasing size is connected later to realize additional feature extraction under different scales. Finally, the regression method is used to obtain the category and location of the target.
2.3. Security assertion markup language

The SAML specification defines three roles: principal, identity provider, and service providers. As can be seen from the Figure 3, the principal requests a service from a service provider. The service provider requests the identity provider and gets an identity assertion from there. Before sending an identity assertion to a service provider, the identity provider asks the principal for information, such as a username and password, to verify the legitimacy of the principal's identity.

3. The proposed Method

3.1. Overall framework

In order to achieve effective protection of sensitive image information, this paper proposes an access control mechanism based on image content recognition and user identity level. The access mechanism includes the identification, location and access of image sensitive areas, which combines classification, target detection in deep learning and SAML techniques. Based on image content and user level, a binary tree structure access strategy is proposed.

Figure 4 shows the overall framework of the access control mechanism, which includes three roles:
Figure 4. Overall framework of access control mechanisms

1) Image Provider: The owner of the image. In order to achieve hierarchical management of sensitive image regions, the data owner defines the image sensitivity level according to the image content; the defined sensitivity level and all image samples are transmitted to the access controller for processing. In this article, the image owner does not have access policy creation rights and is implemented by a separate module.

2) Image Visitor: Request image resources. The image resource is obtained from the access controller, but the acquired image content depends on the level of the visitor.

3) Access controller: The main part of the framework. The role is to achieve hierarchical classification, encrypted storage, access policy, user identity analysis and image distribution of sensitive images. This paper divides it into four functional modules:
   ① Image Processing Module: Accurate identification and positioning of sensitive areas are the premise of implementing hierarchical management and access. The module recognizes different levels of sensitive areas in the image and obtains its specific coordinate position. In order to protect the security of sensitive image data, the sensitive areas in the image are encrypted. Upload the encrypted image to the image management and distribution module, allowing the remaining users to share and access within the scope of the authority.
   ② Strategy Formulation Module: Develop an access strategy. This strategy depends not only on the identity level of the accessing user, but also on the level of sensitive areas in the image. Both the requesting service provider and the service provider implement hierarchical management, and the rights are mapped according to the level of both parties.
   ③ User Control Module: It is mainly responsible for legality authentication and identity analysis of the user identity, and the assertion information of the identity level is used as the only attribute for confirming the user rights.
   ④ Image Management and Distribution Module: grasp the identity level of the visitor, process the image information according to the access policy, and distribute the image for the data visitor. Visitors can only get the image area allowed within the scope of the permission, so the visitor does not surely get a complete image.

3.2. Scheme construction

3.2.1. Level Definition. An image is often treated as an object, but there are also sensitive areas and non-sensitive areas in a single image. All areas of the image are stored and managed without distinction, resulting in a large waste of resources. Therefore, in this paper, different sensitivity levels are determined for a single image according to the image content, realizing hierarchical management of the image.

The basis for the definition of sensitivity is the loss caused by the leakage of the image area, the value of the image information or the importance to the owner of the image [10]. As shown in Equation (1), this paper divides the image sensitivity into four levels, and the sensitivity decreases in turn, indicating: high sensitivity, medium sensitivity, low sensitivity, and non-sensitivity.
Sensitivity _ level = \{s_3, s_2, s_1, s_0\}

As shown in Equation (2), all legal users are divided into four levels, including high-level users, medium-level users, low-level users, and ordinary users. The larger the subscript, the higher the level.

User _ level = \{u_3, u_2, u_1, u_0\}

3.2.2. Access strategy development. The development of an access policy depends not only on the user's identity level, but also on the sensitivity level of the image information. Both the visitor and the accessed data are hierarchically managed, and the two levels are mapped one by one to construct an access policy of the binary tree structure.

\[
\text{Access \_ strategy} = \begin{cases}
(s_0), & \text{if} (\text{user \_ level} = u_0) \\
(s_0, s_1), & \text{if} (\text{user \_ level} = u_1) \\
(s_0, s_1, s_2), & \text{if} (\text{user \_ level} = u_2) \\
(s_0, s_1, s_2, s_3), & \text{if} (\text{user \_ level} = u_3) \\
\emptyset, & \text{else}
\end{cases}
\]

The normal user u_0 can only access the non-sensitive area s_0 in the image. The low-level user u_1 has the authority of the ordinary user u_0, in addition to accessing the low-sensitivity image s_1 area in the image. In other words, the low-level user u_1 can access the non-sensitive image area s_0 and the low-sensitivity image area s_1 in the image. And so on, constitute a binary tree structure access strategy as shown in Figure 5.

![Figure 5. Access strategy with binary tree structure](image.png)

3.2.3. Identification, Location and Encryption of Sensitive Areas. The detection and localization of the sensitive area of the image is to excavate the sensitive area in the image, determine the sensitivity level, and obtain its specific coordinate position. The process involves image detection and target positioning. This paper uses the Mobilenet_ssd model proposed by Howard [11] in 2017 to realize the recognition and location of sensitive areas. Based on the SSD model, the model uses the Mobilenet network to replace the VGG network as the basic network, and connects 8 convolutional layers to form the entire network architecture. It can simultaneously consider the detection speed and accuracy, and realize the identification of sensitive areas. The location of the target area. Then, the identified sensitive image area is subjected to an encryption operation. The specific process is as follows:

1. Image annotation: Determine the sensitive area category in the image, use the tool or autonomous image annotation, frame the target area with closed lines, set the corresponding category labels, and form label text information corresponding to the image one by one.

2. Model construction: The model framework selected in this paper is shown in the following figure. The Mobilenet_ssd model is mainly divided into four parts: the first part is the input module for reading the input image sequence; the second module is the Mobilenet basic network. The function is to realize the feature extraction of the image; the third module is the SSD module, which is used to
identify the sensitive area and determine the location of the sensitive area; the fourth module is the output module, which will output the image results of positioning and classification.

Figure 6. Network architecture diagram of Mobilenet_ssd model

(3) Model training: model training is performed with the tagged image data set, and the trained model is saved; the model is used to identify and locate all sensitive areas of the sample image.

(4) Image encryption: In order to ensure the security of sensitive images, sensitive areas in the image are encrypted.

(5) Data transmission: Upload the processed image to the trusted data management and distribution module to facilitate access and resource sharing by other users.

3.2.4. User authentication. After receiving an access request from a user, in order to prevent unauthorized access, an identity authentication request is first sent to the access user to verify whether it is a legitimate user. The user submits personal attribute information to verify whether the user exists in the user list. If it does not exist, the user’s resource access request is rejected. Otherwise, the user is further analyzed for identity level and the identity level of the accessed user is determined.

3.2.5. Data distribution. Firstly, get the image that the user wants to access. The image is then processed based on the access policy and the identity information of the user. The sensitive image area allowed to be accessed within the user level is decrypted, the unreachable area is still encrypted, and the image is distributed to the visitor.

4. Result and discussion

4.1. Experiment

4.1.1. Dataset. This paper uses the student I.D. image in the student management system as experimental data. The student I.D. image usually contains information such as the student's photo, student ID, identity number, name, degree, major, and birthplace. In this paper, the face image is divided into high-sensitivity levels, the name and birthplace are set to medium sensitivity, the student number is low sensitivity, and the rest of the information belongs to the non-sensitive image area. Use the tool to mark sensitive areas and grade labels in the image to form an annotation file corresponding to the image.

4.1.2. Identification of Sensitive Areas. Train the constructed mobilenet_ssd model on the dataset to detect and locate sensitive areas in the image. The results of the sensitive area detection are shown in Figure 7.

4.1.3. Image Encryption. In order to realize the protection of the sensitive image area, the location of the sensitive area is obtained according to the specific coordinate information of the positioning, and the encryption operation is performed as shown in Figure 8.
4.1.4. Access Image Results. When a visitor requests to access an image, the content of the picture that can be accessed by different identities is as shown in the following figure. The high-level user can access the complete picture information, and the middle-level user can access the image information except the high-sensitivity area, and the low-level user is low. Sensitivity areas and non-sensitive areas have access rights, while normal users can only access non-sensitive area images.

Figure 9. Images accessed by users of different identity levels. The Figure on the left of the first line is the image obtained by the no-grade users, the right is the figure seen by the low-level users. The two pictures in the second line are the perspectives of medium-level users and high-level users.

4.2. Method analysis

4.2.1. Functional separation. The right to develop an access policy is separated and given to the independent module operation, not the image owner. Only the users who meet the requirements can obtain the corresponding data, and the security is higher.

4.2.2. Fine-grained. The user performs hierarchical management based on the level, the image resources are classified according to the sensitivity, and the access subject and the object are hierarchically managed. Users of the i level can only access the image areas of the sensitivity level i and below i, achieving fine-grained access to image data.
4.2.3. **Confidentiality.** The image sensitive area is encrypted and stored, and even if it is maliciously leaked, it is only a non-sensitive area, which effectively protects the security of the sensitive image area.

4.2.4. **Locality.** The single image is divided into different regions based on the sensitivity, instead of the single image as a whole, the local processing and management of the image is realized.

5. Conclusion

In order to realize data privacy and secure access of sensitive images, this paper proposes an access control mechanism based on image recognition and user identity. The mechanism is based on the sensitivity level, hierarchically manages the image, and combines the user's identity level, thus achieving fine-grained access control for different sensitivity image areas, and effectively ensuring the security of sensitive image information.

The subsequent scheme can further study and discuss the fine-grained access control of complex images and sensitive image protection in cloud environments.

**Acknowledgments**

This research is funded by the State Grid Ningbo Power Supply Company Innovation Consulting Project--Research on Intelligent Detection and Verification Technology for Power Information Network Security Hidden Trouble.

**References**

[1] Ma X.T. Research on Multi-Dimensional Sensitive Data Protection of Library Big Data Platform [J]. Library, 2017, (2): 70-75.

[2] CHI Y.P, WANG Y, WANG H.L, et al. Cross-domain access control for e-government cloud based on classification [J]. Computer Application, 2016, (2): 402-407.

[3] SHAO Y.W, ZHAO Y.M. Hierarchical attribute-based key exchange in cloud computing [J]. Computer Applications & Software, 2018, 35(8): 314-319.

[4] YAN X.X, GENG T. Fused access control scheme for sensitive data sharing[J]. Journal of Communications, 2014, 35(8): 71-77.DOI: 10. 3969/ j.issn.1000-436x.2014.08.010

[5] State Grid Corporation, China Electric Power Research Institute, State Grid Shanghai Electric Power Company. A Sensitive Image Recognition Method in Internal and External Interaction of Power Network: China, CN201310627243.3 [P].2014-02-26.

[6] HOWARD A.G, ZHU M, CHEN B, et al. MobileNets: efficient convolutional neural networks for mobile vision applications [J/OL]. ARxiv:1704.048612017-0417] https://arxiv.org/abs/1704.04861.

[7] FAN J.C. Study on Classification and Recognition of Orchard Pests Based on MobileNets[J]. Tianjin Agricultural Sciences, 2018, 24(9):11-13,26.

[8] Liu W, Anguelov D, Erhan D, et al. SSD: Single shot multibox detector[C]. Lecture Notes in Computer Science,2016.

[9] TONG X, ZHANG J. Object Detection of ROS Platform Based on SSD_MobileNet Model [J]. Computer Systems & Applications, 2019, 28(01):94-99.

[10] LIU M.H, ZHANG N, ZHANG Y.Y. Research on Sensitive Data Protection Technology on Cloud Computing [J]. Telecommunications Science, 2014, 30(11): 1-8. DOI: 10.3969/j.issn.1000-0801.2014.11.001.

[11] Howard AG, Zhu ML, Chen B, et al. MobileNets: Efficient convolutional neural networks for mobile vision applications. arXiv preprint arXiv: 1704.0486,2017.