Fine-grained Image Authorization Mechanism for Image Management Systems

Yi-Hui Chen[1,2], Eric Jui-Lin Lu[3], Ping-Jung Chen[3]

[1] Department of M-Commerce and Multimedia Applications, Asia University, Taiwan
[2] Department of Medical Research, China Medical University Hospital, China Medical University, Taiwan
[3] Department of Management Information Systems, National Chung Hsing University, Taiwan
chenyh@asia.edu.tw, jllu@nchu.edu.tw, karenchen87@gmail.com

Abstract

To protect personal privacy and confidential preservation, access control is used to authorize legal users for safe browsing the authorized contents on photos. The access control generates an authorization rule according to each permission assignment. With low maintenance loads, this paper integrates the PM-tree compression and access control technique to propose a fine-grained access control model for digital image systems. The proposed scheme enables users to have different views of an image after they login to the system. The authorization unit for the image can be parts of the image, such as a pixel, a block, several blocks or the whole image. The experiments implement this model on the Blueprint Collaboration System (BCS) provided the positive data to confirm its feasibility.

Keywords: Image access control, Fine-grained access control model, Confidential preservation

1 Introduction

In recent years, people used to obtain and store information on the Internet with the onset of the widespread use of network technologies. The Internet is a public, but insecure environment, which might make user's private information vulnerable to malicious intruders during data transmission. To ensure that no illegal users can access the unauthorized contents, access control model [1] is a kind of security mechanism to authorize different authorizations to different users according to their own permissions. The original purpose of access control is from the management of the massive data; that is, some secret data may allow being accessed by a specific user, and permissions of users are different. Using the model, users can authorize people who have rights to access their own digitized contents. After that, users can be granted or denied to resources after they login to the systems. Access control can be applied to several domains, such as cloud [6, 31] mobile [30], wireless cellular networks [19], database [1] and so on.

In regular access control model, all the information is centralized to store at a server. The information outsourcing and stored to a third party, but it never guarantees whether the third party is trust. To eliminate the risk of the un-trust third party, blockchain technology provides peer-to-peer security and encryption thanks to its distributed nature. Applying blockchain technology to access control model [32], all the information is distributed and is not stored at the centralized third party. An end user could be able to select which personal data to share in the network because all the end devices act autonomously. Blockchain access control technology is a new brand technique in authorization model.

Nowadays, the massive use of multimedia causes several issues to arise including privacy and preserving confidentiality. Accessing control models for multimedia databases [1-8], [16-22, 29] are proposed to provide safe browsing and publishing of multimedia. In 2003, Bertino et al. [8] proposed a hierarchical access control model for video database systems. Based on hierarchical concepts, Thuraninsigham [28] created a digest between the content of the video and the corresponding description to facilitate the specification of permissions. Pickering et al. [23] prevented illegal copying by controlling the quality of videos. Later on, as for the quality of services (QoS), Grosbois et al. [16] and Phadikar et al. [22] proposed schemes to modify the DWT (Discrete Wavelet Transform) coefficients and DCT (Discrete Cosine Transform) coefficients for providing different resolutions and qualities of images to different users. In [1], Nabil R. Adam et al. proposed an access control model dedicated to the protection of digital libraries' contents. In [3], Atluri and Chun proposed an access control model for geospatial data. Imaizumi et al. [17] proposed a multi-layers encryption mechanism for JPEG2000 images used in privacy protection. However, all of them focused on accessing a whole digitalized

[*] Corresponding Author: Eric Jui-Lin Lu; E-mail: jllu@nchu.edu.tw

DOI: 10.3966/160792642018111906027

content, but not allowing access to just partial contents.

The control of partial contents in multimedia has been an important issue in recent years, named fine-grained access control (e.g., masking out objects with violent scenes for a TV show, hiding the sensitive information in a picture) [5]. That is, one may prefer to access the partial contents of an image rather than to the entire one for privacy protection such as some leading services (e.g., Google Street View, EveryScape, and Mapjack), personal image management, marketing promotion, etc. Google Street View provides users to see the street view after they look up the location in the map; however, the service results in a high probability of leaking one's private life without meaning to do so [2]. This has raised a need to de-identify individuals from the view of the street, but not encrypt the whole content of images. Also, it is useful for personal image management to just encrypt the sensitive regions of images as random pads. It is a benefit that the owner can see the non-sensitive region to recognize which pictures he looks for. Second, only the user who has rights can decrypt the encrypted regions to prevent personal privacy leakage. As for marketing promotion on electronic publications, the partial interest words of bubbles or patterns in e-comics can be encrypted as random pads to attract readers to know what meaning is contained in the pictures [24].

As for fine-grained access control for digitalized multimedia, Bouna et al. [5] proposed an image access control model, which enables owners to authorize the partial contents of an image to users. The fine-grained access control model can specify the security rules based on the constraints, which provide a simple data representation model to properly describe the image description, and present the requirement of fine-grained control on the image. There is a challenge that a significantly increasing number of pictures need to be maintained owing to a vast number of authorizations that need to be maintained as well. Pinto et al. [24] change the values of AC coefficients during the JPEG compression process to encrypt just the bubbles of e-comics, namely selective image encryption. After that, the encrypted area can be restored to the original ones if the secret key is held. The partial image encryption has two advantages [24]. First, the computational time can be reduced because only partial contents are required to encrypt. Second, the regions are selected by owners to encrypt partial contents according to their wishes. To achieve partial encryption, Pinto et al. proposed a selective encryption scheme [24], in which the encrypted regions are controlled by coefficients. However, it is not sophisticated; that is, some regions are encrypted but the ones are exactly matched according to the correct ones to-be encrypted as desired. As for publishing, it controls the regions of contents that users can view according to the money they paid. Collaboration is the often the case in recent business models, such as collaborative IC design, so that some regions are core values in the blueprint, but some parts are needed to be designed by outsourcing designers; thus, the limited information is to be provided for outsourcing designers. The simplest way for fine-grained access control is to duplicate and to send several copies to users according to their own permissions. The management cost is very high because the huge quantity of digital images grows increasingly and needs to be managed. It is desirable to have a fine-grained access control for digital images, which can be disabled to see the curial parts of the blueprint. This paper extends the details of the previous work [12] to provide a fine-grained image access control with low cost management, and implements this model on the Blueprint Collaboration System (BCS).

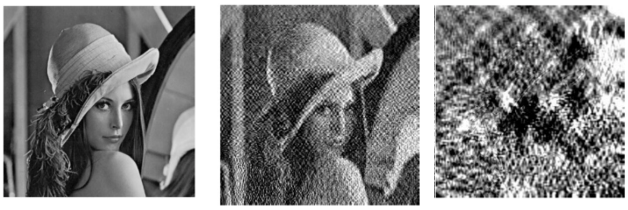
This paper is organized as follows: Related works are briefly described in Section 2. In Section 3, the details of the proposed scheme are presented, including the encryption and decryption procedures. The experimental results are shown in Section 4. Finally, conclusions and directions for future work are drawn in Section 5.

2 The Related Works

In past research, access control is widely used to protect historical medical records [26] and in recently developed cloud computing [33] and wireless sensor network [22]. Most of the current research on access control [9-12, 14] focuses on how to authorize different parts of the contents of a document to different users. Nowadays, image access control is widely used in the QoS (Quality of Services) for wireless communication systems. The quality of images or videos that users can see is based on the money users had paid, and the quality is poor when being accessed by an illegal user [16-22]. The QoS control models for digital images is insufficient for some specific domains, such as publishing [9] and collaboration [13]. This is because most of them focus on how to control for a whole image, but just one in parts of the image.

In recent years, many investigators have reported on access control of images. Grosbois et al. [16] proposed the authentication and access control mechanism on the converted image using DWT. The mechanism can control the resolution and quality of the image. Imaizumi et al. [17] proposed a hierarchical encryption scheme for JEPG2000 code streams. The master key can generate several keys, and a different key is delivered for a user permitted to access a different quality. Pickering et al. [23] embed the watermarks into the digital video using the Dual-Tree Complex Wavelet Transform to provide efficient access control of digital video. Phadikar et al. [22] proposed a method of quality control that adapted to the converted gray image using DCT. It adjusts the DC value that is converted by DCT to control the quality of image. Atluri and Chun proposed a geospatial data authorization model (GSAM) [3] for the spatial and temporal attributes of data, such as location, resolution, and the time of image downloads, etc. As for TV shows, it masks out objects with violent scenes to hide the sensitive information in a video frame [5]. Ma et al. [17] proposed a fine-grained access control on spatial data in the grid environment. Also, Zeng et al. [33] proposed a secure access mechanism for a spatial database.

This research is widely used in the QoS of wireless communication systems. The quality of images and videos that users can see is based on the money users have paid, so it can prevent illegal copying using poor quality images. For example, Figure 1(a) is the original image, and Figure 1(b) is the low quality image. Figure 1(c) is the image quality for illegal access.



(a) Original image (b) Low quality (c) Illegal access

Figure 1. Image access control on the QoS [22]

The past methods focused on the quality management of the whole image, but these methods cannot be used in fine-grained image access control, namely cannot provide the mechanism for authorizing different user different authorization regions of the same image. Bouna and Chbeir [4] proposed the fine-grained access control for digital image that applied on the image database and surveillance system. It aims to protect the interested data(s) of images using blurs, so that only authorized users can access the authorized data. Deciding whether the user is legal will be compared to the photo shot by the web camera with the image stored in the image database. There is no need to say that it requires a large amount of time to search the entire database for image comparison. Zeng et al. [33] proposed a role-based access control model on geographical databases. In this scheme [33], users should register their account and related information on the system, such as name, password, authorized codes, role, and so on. Later on, the server authenticates the credentials of the user and authorizes his/her own authorized views after the user logins to the system. Ma et al. based on RBAC (Role-based access control), a concept to propose a fine-grained security access control model. The scheme [27] is also for geographical database to limit users to access some specific regions of the maps. In this scheme [3], the GSAM (Geospatial Data Authorization Model) is proposed to manage the authorization assignments according to timestamps, credentials of users and authorized regions.

3 The Proposed Scheme

The details of the FGAC-Processor design are shown in Figure 2. The design allows different users access to different regions in the same image. In Figure 2, after the FGAC-Processor gets the commands from users sent to the server, the processor authenticates the credentials of users via the "User Information" file. The user information collects the credentials of users for authenticating whether they are legal users. If passing the authentication, the rules extracted from file "Authorization Rules" are used to match the users' authorizations. The authorization rules are the rules for recording who has which rights to access which parts of the objects. Finally, the authorized views are generated through the FGAC-Processor. The FGAC-Processor is demonstrated with First Order Logic 0 as shown in Section 3.2.2, and the corresponding development is shown in Section 3.2.3. In addition, the authorized regions must be described in the authorization rules, and illustrated in Section 3.1.

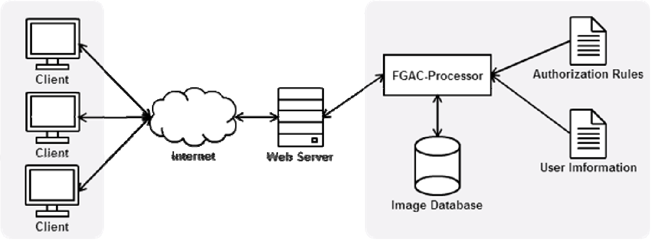


Figure 2. The flowchart of the FGAC-Processor access control system

3.1 ROI Region

In the proposed method, the different users probably have different authorized regions. An authorization rule includes the authorized user, the authorized object and authorized contents. The authorized object is an image, the content is the region of the image that is authorized to the user with rights to access, namely ROI (Region of Interest) region.

Taking Figure 3 as an example, the group of pixels can be access and marked with 1, namely the pixel is ROI; otherwise, 0 represents that the pixels that are disabled from access, are called the non-ROI region. Generally, the pixels in a ROI region are adjacent and continuous; thus, it can be compressed by using the PM-tree (Peano Mask Tree) [14]. After that, the compressed codes are treated as the authorized content.

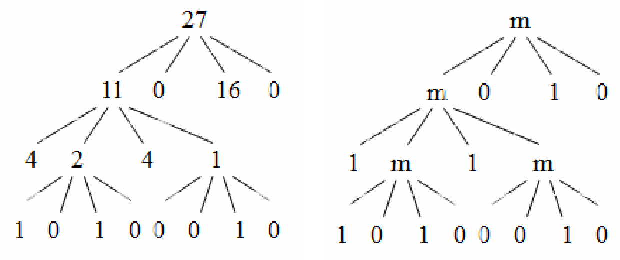
1	1	1	0	0	0	0	0
1	1	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0

Figure 3. An authorization region example for a given image with a size of 8×8

Figure 4 is a dimensional matrix including 0s and 1s, which can be seen as a quad tree using the P-tree (Peano Count Tree), as shown in Figure 4(a). The P-tree can be compressed to be PM-tree and is described below.

First, the root of P-tree R_0 is the number of 1s in the matrix, and then the matrix is cut into four pieces equally. Four nodes of the first level are called R_1, R_2, R_3 and R_4 to keep the number of 1s individually. If the number of 1s is zero or the same size of the piece, the piece does not need be cut anymore; otherwise, it will continue to break out until the size of the piece is equal to one.

Then, it converts the P-tree into the PM-tree as shown in Figure 4(b). The non-terminal nodes are replaced with m. Moreover, the values of the leaf nodes are larger than 1, they are replaced with 1.



(a) P-tree (b) PM-tree

Figure 4. Examples of P-tree and PM-tree after compressing Figure 2

Later on, the PM-tree is visited using a preorder to generate a bit string. If the value of the node is m, then it returns "1*m*". If the value of node is 0 or 1, add "0" in front of the value, and it returns it. That is, if the value is 0, the returned value will be "00". If the height of the node is the same as the height of tree log4n, it returns the value of the node directly, where n is the size of matrix. The final output string is called the ROI Path. For example, the ROI Path of Figure 4(b) is "1*m*1*m*011*m*1010011*m*0010000100". Figure 5 is the pseudo codes of the compression process. In Figure 5, the main function calls the method Region_To_Path (,,,) for the authorized image, in which the parameters are the first pixel at the coordinates (s_x, s_y) and the last pixel at the coordinates (e_x, e_y). The sensitiveRegion Array matrix is used to record whether the region is a ROI (or non-ROI) region. The matrix is composed of 0s and 1s, which represent the non-ROI region and ROI region respectively. The count is a variable to accumulate the value equal to 1 in the sensitiveRegion Array when using the function. CulSizeOfRegion(). AreaSize() is a function to return the size of the sensitiveRegionArray. In the ROI_To_Path(,,,) function, the input data are the start coordinates and end coordinates of an image and the imageROIArray. It would output the ROI path whose type is string. The possible results of the function Region_To_Path (,,,) are listed below: (1) the entire region is the ROI region so that all the values are equal to 1 in the sensitive RegionArray matrix. If the size of the image region is 1,

```
public static void main (){
        //($s_x$, $s_y$) are the start ($x$, $y$)-coordination
        //($e_x$, $e_y$) are the end ($x$, $y$)-coordination
String authorized_path=Region_To_Path($s_x$,$s_y$,$e_x$,$e_y$);
}
//sensitiveRegionArray are the array to record the region
grant and denied, which marked with 1 and 0.
String Region_To_Path (int $s_x$, int $s_y$, int $e_x$, int $e_y$) {
        int count = 0;
        // CulSizeOfRegion() is a function to accumulate the
           value equal to 1 in sensitiveRegionArray
        // AreaSize() is a function to return the size of
           sensitiveRegionArray
           count= CulSizeOfRegion (sensitiveRegionArray);
           area = AreaSize(sensitiveRegionArray);
           if (count ==area) {
              if (area== 1) {
                 return "1";
              } else {
                 return "01";
              }
           } else if (count == 0) {
              if (area== 1) {
                 return "0";
              } else {
                 return "00";
              }
           } else {
//The recursive process is to slice the
//sensitiveRegionArray into four equivalent //pieces and to
be processed again till the region //is fallen into the first or
the second case.
         return "1m" + Region_To_Path ($s_x$, $s_y$, $s_x$+($e_x$-$s_x$+1)/2,
$s_y$+($e_y$-$s_y$+1)/2)
            + Region_To_Path ($s_x$+($e_x$-$s_x$+1)/2, $s_y$, $e_x$, $s_y$+
($e_y$-$s_y$+1)/2)
             + Region_To_Path ($s_x$, $s_y$+($e_y$-$s_y$+1)/2, $s_x$+
($e_x$-$s_x$+1)/2, $e_y$)
             + Region_To_Path ($s_x$+($e_x$-$s_x$+1)/2, $s_y$+($e_y$-$s_y$+1)/2,
$e_x$, $e_y$);
           }
}
```

Figure 5. The pseudo code of the AR Path for compressing the authorized regions

the node is a leaf node; otherwise, non-leaf node. In this case, the leaf node and non-leaf node are marked as 1 and 01, respectively. That is, if the number of pixels in the ROI region is the same as the size of the input range which is equal to 1, returns string “1”; otherwise, if the value is larger than 1, it returns “01”. (2) If the entire region is a non-ROI region, all values are marked as 0. If the size of the region is larger than 1, it is a non-leaf node; otherwise, leaf node. In this case, the returned values for the leaf node and non-leaf node are 0 and 00, respectively. That is, if the size of the input region is 1, it returns string “0”; otherwise, it returns “00”. (3) If the number of pixels in the ROI region is neither the size of the input region nor 0, return “1m”and four strings which are generated from calling itself recursively and whose input regions are to cut the original input region into four pieces equally.

3.2 First Order Logic Model

The main factors of access control are the subject, object, and action. The subject represents the set of users as shown in Eq. (1), where U is the set of all users and n is the number of users.

$$U = \{u_i \mid 1 \le i \le n, n\ is\ the\ number\ of\ users\} \quad \textbf{(1)}$$

The object is an image, a block of the image or a pixel in the image as shown in Eq. (2), where o_{ij} indicates the j-th authorized region of the i-th image. O_i set is all the authorized regions of the i-th image and t is the number of the authorized regions. In Eq. (3), the i-th image is the union set of all authorized regions as O_i. In Eq. (4), O is the set of the authorized region O_i, where m is the number of images. In the fine-grained access control model, the authorized object is o_{ij}. As shown in Figure 6, two ROI regions and one non-ROI region are denoted as o_{11} and o_{12}, and o_{13}, respectively. Three authorized regions o_{11}, o_{12}, and o_{13} are union as represented by O_1. Action is what the user can do on the authorization region, such as read, edit, etc. The types of actions are read and modify as shown in Eq. (5).

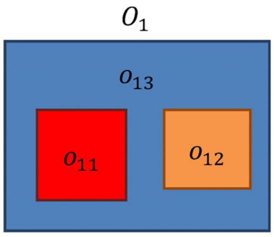


Figure 6. Example of O_1 and its authorized regions

$$O_i = \{o_{ij} \mid 1 \le j \le y, t\ is\ the\ number\ of\ ARs\ in\ O_i\} \quad \textbf{(2)}$$

$$\bigcup_{j=1}^{t} o_{ij} = O_i \quad \textbf{(3)}$$

$$O = \{O_i \mid 1 \le i \le m, m\ is\ the\ number\ of\ images\} \quad \textbf{(4)}$$

$$A = \{\text{“}ready\text{”}, \text{“}modify\text{”}\} \quad \textbf{(5)}$$

In Eq. (6), AUTH is the assignment related to authorized region, users, and action. In Eq. (7), the function authorized_regions („) inputs the subject (u), object (O_i) and action (a) to present all the authorized regions assigned to the user u.

$$AUTH \subseteq U \times O_i \times A\ for\ 1 \le i \le m \quad \textbf{(6)}$$

$$\begin{aligned} &authorized\_regions(u, O_i, a) \\ &= \{o_{ij} \mid (u, o_{ij}, a) \in AUTH \cap o_{ij} \in O_i\} \end{aligned} \quad \textbf{(7)}$$

In Eq. (8), $Rule_A$ is the authorized rule of the FGAC access control model to allow user u to authorize o_{ij} with action a.

$$Rule_A : allow(u, o_{ij}, a) \leftarrow o_{ij} authorized\_regions(u, O_i, a) \ \textbf{(8)}$$

3.3 Example of First Order Logic Model

The above model can be implemented in any access control system. Take the XML access control as example shown in Figure 7 and its corresponding DTD scheme as shown in Figure 8. The element Policy_base includes child elements Policy_spec which is the authorization rule. Attributes of Policy_spec such as cred_expr, target, path and auth are user name, location of image file, ROI path and authorized action respectively.

```
<?xml version=“1.0” encoding=“UTF-8”?>
<!DOCTYPE Policy_base SYSTEM “RoleAccessControl.
dtd”>
<Policy_base>
<Policy_spec target=“Blueprint1.raw”
path=“1m1m011m1010011m0010000100” cred_expr=
“Alice” auth=“Read”/>
</Policy_base>
```

Figure 7. XML example file based on the first order logic model

```
<!ELEMENT Policy_base (Policy_spec+)>
<!ELEMENT Policy_spec EMPTY>
<!ATTLIST Policy_spec cred_expr CDATA #REQUIRED>
<!ATTLIST Policy_spec target CDATA #REQUIRED>
<!ATTLIST Policy_spec path CDATA #REQUIRED>
<!ATTLIST Policy_spec auth CDATA #REQUIRED>
```

Figure 8. DTD of the first order logic model

4 Experimental Results

This experiment aims to build a Blueprint Collaboration System (BCS). The system is used as a collaborative design of an interior blueprint and implements the model by using NetBeans 6.5 and Java Standard Edition 1.7 of Oracle.

The fine-grained image access control in Section 3 can apply to many environments easily such as relational database and XML. The BCS implements a fine-grained access control on the XML to record the user's authorizations. The original image is shown in Figure 9 (take file name Blueprint_B110412 for example). After logging in to the BCS as in Figure 10, the BCS list images that users can access in his/her drop down list based on the user's authorizations. In Figure 11, the user is able to browse and to choose the image under their authorizations. After selecting one of the choices in the list, the panel shows the blueprint as shown in Figure 11. The user can read or edit authorized regions as follows: user can "read" in the blue part and "edit" in the white part. The tool package on the left side can be used to draw and design the ROI regions in which the authorized action is edit.

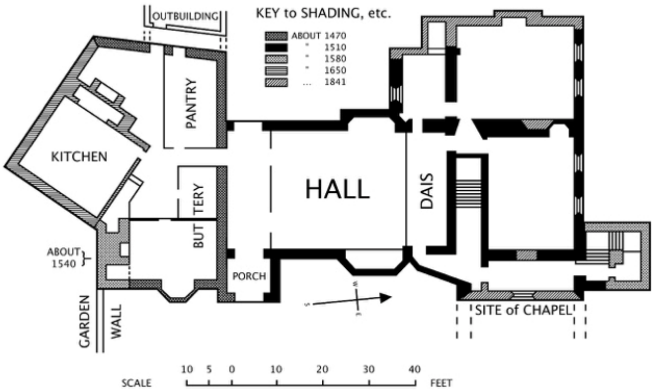


Figure 7. The original image of Blueprint_B110412 [25]

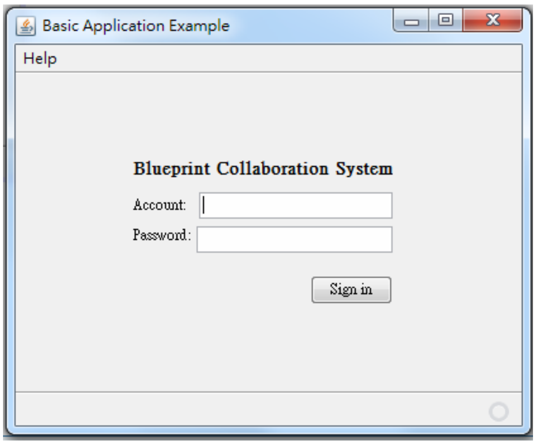


Figure 8. The welcome view of the prototype system

There are five blueprints and five users using BCS now, three are designers and two are builders. Each designer has different ROI regions of the action "edit" and the action "read" in every single blueprint. Figure 12 and Figure 13 are snapshots while designer Alice and Bob are designing the file "Blueprint_B110412". Although they open same file, the regions they can see are different. Builders only have action "read", and have different regions that are authorized in each blueprint as shown in Figure 14. In the BCS, the elements in the number of ((3×2+2×1)×5) can be created in an XML file, which instead of the (3×2+2×1)×5, images are generated by using the traditional method. As can be known from the above result, the maintenance cost and space complexity using the method proposed by this paper are significantly less than using traditional methods.

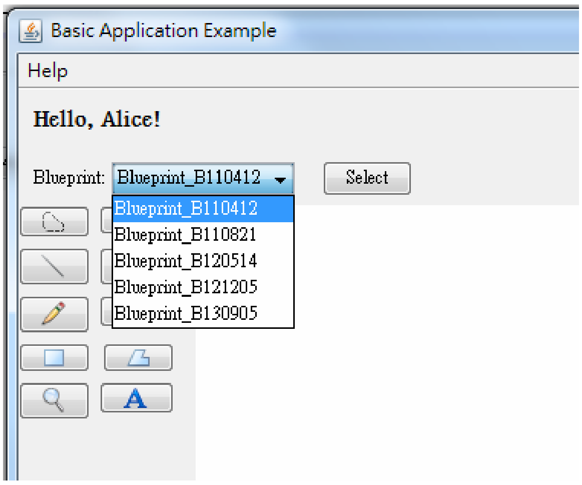


Figure 9. The selection of authorized objects

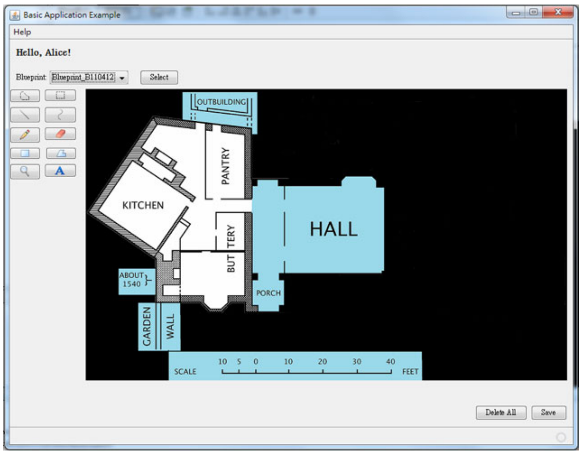


Figure 10. The authorized view of designer Alice

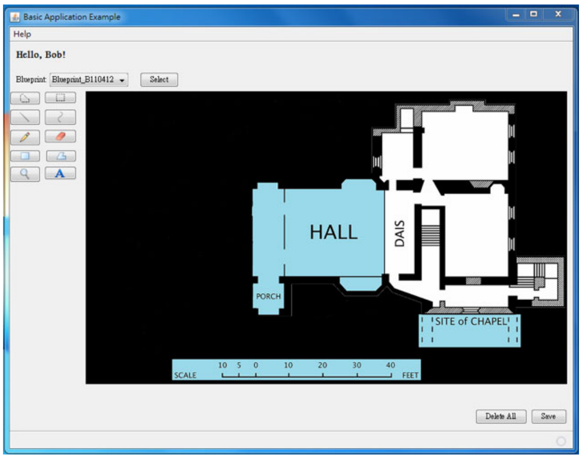
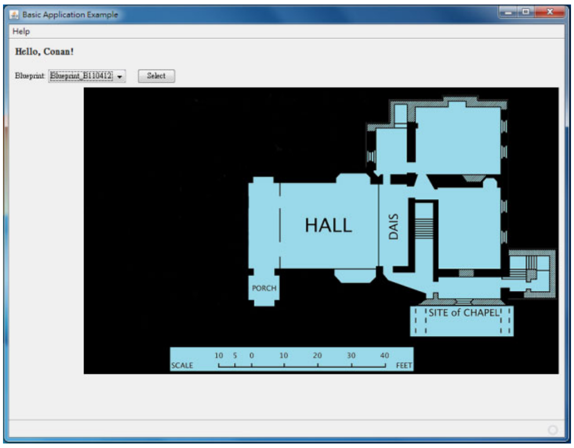


Figure 11. The authorized view of designer Bob



Hello, Conan!

Blueprint: Blueprint_B110412

Figure 12. The authorized view of builder Conan

To summarize the advantages of the proposed scheme when compared to the others, are listed in Table 1. The FGAC model allows different users with different permissions to access the same objects or different objects. Bouna et al. [5] proposed the fine-grained access control on a surveillance system to enable users with read action. Also, Ma et al. [18] proposed fine-grained access control, but permission assignment is inflexible. The object authorized by Atluri et al.'s scheme [3] must be a regular pattern or shape, but not supporting the irregular shape. Also, the Zeng et al.'s scheme [33] does not support an irregular authorized region as well as flexible authorizations. In the proposed scheme, the irregular shape can be resolved by using the AR Path and the authorization is more flexible to support not only read, but also modify action.

Table 1. The performances of the proposed scheme compared to the other ones

Compared methods	Flexible authorizati on	Fine-grained access control	Irregular authorized region supporting	Read and write actions supporting
[5]	✓	✓	✓	
[33]	✓	✓		
[18]	✓	✓	✓	
[3]	✓	✓		✓
Proposed	✓	✓	✓	✓

5 Conclusions

This paper proposes an image fine-grained access control model appropriate to a collaborated design. To make image fine-grained access control a reality, the ROI regions of an image are compressed to convert into a PM-Tree as a ROI Path. A prototype system, Blueprint Collaboration System, is implemented by using XML files to allow different users to have different permissions to access the image. In future works, we are planning to add a role-based authorization concept to the proposed scheme. This will allow a person who inherits a higher role to have permission to see lower ones. Additionally, we would like to add a hierarchical concept to the ACTION part if the ROI regions are overlapped, but different actions are authorized. In the future, we shall try this method when applying to other applications, such as personal image management. Some issues related to access control (e.g., delegation, federate cooperation, etc) would be examined in the near future.

Acknowledgments

We thank the Ministry of Science and Technology for supporting this research with IDs MOST 106-2221-E-468-001 and MOST 106-2632-E-468-003. Our gratitude goes to Michael Burton, Asia University

References

[1] N. R. Adam, V. Atluri, E. Bertino, E. Ferrari, Content-ased Authorization Model for Digital Libraries, *IEEE Transactions Knowledge Data Engineering*, Vol. 14, No. 2, pp. 296-315, August, 2002.

[2] P. Agrawal, P. J. Narayanan, Person De-identification in Videos, *IEEE Transactionson Circuits and Systems for Video Technology*, Vol. 21, No. 3, pp. 299-310, March, 2011.

[3] V. Atluri, S. Ae Chun, An Authorization Model for Geospatial Data, *IEEE Transactions on Dependable and Secure Computing*, Vol. 1, No. 4, pp. 238-254, October, 2004.

[4] B. Al Bouna, R. Chbeir, *Content-based Policy Specification for Multimedia Authorization and Access Control Model, Cyber Warfare and Cyber Terrorism*, IGI Global , 2007.

[5] B. Al Bouna, R. Chbeir, P. Capolsini, A Fine-grained Image Access Control Model, *8th International Conference on Signal Image Technology and Internet Based Systems*, Sorrento-Naples, Italy, 2012, pp. 603-612.

[6] M. Beraka, J. A. Muhtadi, Critical Comparison of Access Control Models for Cloud Computing, *Journal of Internet Technology*, Vol. 16, No. 3, pp. 431-442, May, 2015.

[7] E. Bertino, M. A. Hammad, W. G. Aref, A. K. Elmagarmid, Access Control Model for Video Databases, *9th International Conference on Information Knowledge Management*, McLean, VA, 2000, pp. 336-343.

[8] E. Bertino, J. Fan, E. Ferrari, M.-S. Hacid, K. A. Elmagarmid, X. Zhu, A Hierarchical Access Control Model for Video Database Systems, *ACM Transactions on Information Systems*, Vol. 21, No. 2, pp. 155-191, April, 2003.

[9] E. Bertino, S. Castano, E. Ferrar, Securing XML Documents with Author-X, *IEEE Internet Computing*, Vol. 5, No. 3, pp. 21-31, May, 2001.

[10] R. Chand, P. Felber, Scalable Distribution of XML Content with XNET, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, No. 4, pp. 447-461, April, 2008.

[11] C. C. Chang, Y. H. Chen, T. D. Kieu, A Watermarking Technique Using Synonym Substitution for Integrity Protection of XML Documents, *ICIC Express Letters*, Vol. 4,

No.1, pp. 89-94, February, 2010.

[12] Y. H. Chen, E. J. L. Lu, P. J. Chen, Fine-grained Access Control for Digital Image Systems, *2014 International Conference on Information Science, Electronics and Electrical Engineering*, Sapporo, Japan, 2014, pp. 681-685.

[13] E. Damiani, S. D. C. d. Vimercati, S. Paraboschi, P. Samarati, A Fine-grained Access Control System for XML Documents, *ACM Transactions on Information and System Security*, Vol. 5, No. 2, pp. 169-202, May, 2002.

[14] Q. Ding, Q. Ding, W. Perrizo, PARM ― An Efficient Algorithm to Mine Association Rules from Spatial Data, *IEEE Transactions on Systems, Man, and Cybernetics ― Part B: Cybernetics*, Vol. 38, No. 6, pp. 1513-1524, December, 2008.

[15] First order logic, *Wiki Pedia*, https://en.wikipedia.org/wiki/First-order_logic.

[16] R. Grosbois, P. Gerbelot, T. Ebrahimi, Authentication and Access Control in the JPEG 2000 Compressed Domain, *SPIE Proceeding of 46th Annual Meeting Applications of Digital Image Processing XXIV*, San Diego, CA, 2001, pp. 95-104.

[17] S. Imaizumi, O. Watanabe, M. Fujiyoshi, H. Kiya, Generalized Hierarchical Encryption of JPEG 2000 Code Streams for Access Control, *IEEE Proceeding of Conference on Image Processing*, Genoa, Italy, 2005, pp. 1094-1097.

[18] F. Ma, Y. Gao, M. Yan, F. Xu, D. Liu, The Fine-grained Security Access Control of Spatial Data, *18th International Conference on Geoinformatics*, Beijing, China, 2010, pp. 1-4.

[19] J. H. Moon, Y. J. Lim, Overload Control Technique for MTC Communications in Wireless Cellular Networks, *Journal of Internet Technology*, Vol. 19, No. 1, pp. 271-277, January, 2018.

[20] L. Pan, C. N. Zhang, A Web-based Multilayer Access Control Model for Multimedia Applications in MPEG-7, *International Journal of Network Security*, Vol. 4, No. 2, p. 155-165, January, 2007.

[21] L. Pan, C. N. Zhang, A Criterion-based Multilayer Access Control Approach for Multimedia Applications and the Implementation Considerations, *ACM Transactions on Multimedia Computing, Communications, and Applications*, Vol. 5, No. 17, pp. 1-29, November, 2008.

[22] A. Phadikar, M. K. Kundu, S. P. Maity, Quality Access Control of a Compressed Grayscale Image, *Proceeding of Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics*, Hyderabad, India, 2008, pp. 13-19.

[23] M. Pickering, L. E. Coria, P. Nasiopoulos, A Novel Blind Video Watermarking Scheme for Access Control Using Complex Wavelets, *IEEE Proceeding of Conference on Consumer Electronics*, Las Vegas, NV, 2007, pp. 1-2.

[24] M. Pinto, W. Puech, G. Subsol, Protection of JPEG Compressed E-Comic by Selective Encryption, *IEEE Proceeding of Conference on Image Processing*, Melbourne, Australia, 2013, pp. 4588-4592.

[25] T. M. i. Question, *Wikimedia Commons*, http://commons.wikimedia.org/wiki/File:Horham_Hall_blueprint.png.

[26] B. P. Suarez, C. Molina, C. P. Yanez, M. P. D. Reyes, Contextualized Access to Electronical Health Records in Cardiology, *IEEE Transactions on Information Technology in Biomedicine*, Vol. 16, No. 3, pp. 401-412, May, 2012.

[27] M. S. Rajpoot, P. Patel, A Comparative Study on Various Aspects of Security of Geospatial Data, *Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014, pp. 708-712.

[28] B. Thuraisingham, Security and Privacy for Multimedia Database Management Systems, *Multimedia Tools and Applications*, Vol. 33, pp. 13-29, March, 2007.

[29] B. M. Thuraisingham, G. Lavee, E. Bertino, J. Fan, L. Khan, Access Control, *Confidentiality and Privacy for Video Surveillance Databases*, Lake Tahoe, CA, June 2006, pp. 1-10.

[30] S. Tu, Y. F. Huang, C. H. M., S. C. Magurawalage, L. Peng, Z. Zhou, Access Control System Based Cloudlet and ABE on Mobile Cloud, *Journal of Internet Technology*, Vol. 17, No. 7, pp. 1443-1451, December, 2016.

[31] Z. Wan, J. Liu, R. H. Deng, HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing, *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp. 743-754, April, 2012.

[32] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. J. Du, M. Guizani, MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain, *IEEE Access*, Vol. 5, pp. 14757-14767, July, 2017.

[33] Y. H. Zeng, Z. K. Wei, Q. Yin, Research on Spatial Database: A Secure Access Mechanism, *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics*, Hong Kong, China, 2007, pp. 2174-2178.

Biographies

Yi-Hui Chen received her Ph.D. degree in computer science and information engineering. Later on, she worked at Academia Sinica as a post-doctoral fellow. She is now an associate professor at Asia University. Her research interests include multimedia security, semantic web, text mining, and multimedia security.

Eric Jui-Lin Lu received his Ph.D. (Computer Science) at Missouri University of Science and Technology (formerly University of Missouri-Rolla), U.S.A. in 1996. He is currently a professor at National Chung Hsin University. His research interests include machine learning, image and semantic web, and multimedia security.

Ping-Jung Chen received the M.S. degree in Department of Management Information Systems, National Chung Hsing University. His research interests include multimedia security, information security. Now she is working for Trend Micro Inc.