

## Image Forgery Detection Based on Semantics

Yongzhen Ke<sup>1</sup>, Weidong Min<sup>1</sup>, Fan Qin<sup>2\*</sup> and Junjun Shang<sup>1</sup>

<sup>1</sup>*School of Computer Science and Software Engineering, Tianjin Polytechnic University, China*

<sup>2</sup>*Department of Logistics Management, Nankai University, China*

*keyongzhen@tjpu.edu.cn, fannq@163.com*

### Abstract

*The development of powerful image editing software has made it easy to create visually convincing digital image forgeries. Recently some research works based on general low-level visual features in the field of digital image forensics have been conducted to address this problem. However, there has been little work by analyzing the high-level semantic content of the image. This paper discusses the forgery detection problem of digital image from the point of high-level semantic, and proposes the framework of image forgery detection based on semantics. The framework consists of three components including image recognition, semantic logic reasoning engine and generation of semantic rule. A new fuzzy logic semantic reasoning model for image forgery detection is proposed in this paper. Our reasoning model based on fuzzy logic can give the deterministic and uncertainty reasoning results. Based on the proposed framework of image forgery detection, the prototype system of image forgery detection based on semantics is completed using MATLAB, MySQL database software and ontology software protégé and has the ability to detect abnormal splicing from the foreground and background, avoiding detection using the traditional methods based on low-level image features. Experimental results show that the framework and logic semantic reasoning model for image forgery detection are effective.*

**Keywords:** *Semantic Reasoning, Fuzzy Logic, Protégé, Ontology, Image Recognition, Image Forensic*

### 1. Introduction

With the advent of the Internet and low-price digital cameras, as well as powerful image editing software (such as Adobe Photoshop and Illustrator), ordinary users have more access to the tools of digital doctoring than ever before. It becomes more and more important to devise and deploy efficient and effective approaches to detect such image forgery [1]. In general, image tampering detection approaches rely on analyzing several properties such as: detection of cloned regions [2], analysis of feature variations collected from sets of original and tampered scenes [3], inconsistencies in the features [4], inconsistencies regarding the acquisition process [5-7], or even structural inconsistencies present in targeted attacks [8]. These proposed detection approaches are mainly based on general low-level visual features such as color, shape, texture, light, etc. Analyzing the high-level semantic content of the

image can also have a crucial role in image forgery detection. Because each real image is an organic whole, involved a certain degree of significance, and forgery images combined with different photos express a fictional content, analyzing information related to the image, such as season climate, physical environment, clothing, facial expressions, movements and so on, to judge the authenticity of the images are feasible.

Although many image retrieval methods based on image semantics and semantic logic reasoning theory have been proposed, there is little research on image forgery detection based on high-level semantic information. Inspired by Sangwon Lee [9], this paper put forward a semantic based framework of image forgery detection combining with image recognition, ontology and common sense reasoning technologies. The framework consists of three components including image recognition, semantic logic reasoning engine and generation of semantic rules. Firstly, semantic information of the ontology and its relationship is extracted from the real image dataset and stored as common sense knowledge base used in next step of semantic logic reasoning. Secondly, the recognition result for the testing image through image segmentation and image recognition is used as input of logic reasoning. Last, image forgery detection is completed based on semantic rule, commonsense knowledge base and result of image recognition from testing image.

This paper is organized as follows. Section 2 presents the related works. A framework of image forgery detection based on semantic is described in Section 3. Section 4 presents a fuzzy logic semantic reasoning model for image forgery detection concrete. Experimental procedure and results are discussed in Section 5. Finally, conclusion and future work are drawn in Section 6.

## 2. Related Work

Fridrich *et al.*, proposed a faster and more robust approach for detecting duplicated regions in images [10]. The authors use a sliding window over the image and calculate the discrete cosine transform (DCT) for each region. Each calculated DCT window is stored row-wise in a matrix. In order to perform matching for non-exact cloned regions, lexicographically sorting matrix and searching for similar rows are finished. Johnson and Farid investigated lighting inconsistencies across specular highlights on the eyes to identify composites of people [11]. The position of a specular highlight is determined by the relative positions of the light source, the reflective surface and the viewer (or camera). According to the authors, specular highlights that appear on the eye are a powerful clue as to the shape, color, and location of the light source(s). Inconsistencies in these properties of the light can be used as telltales of tampering. Ng and Chang proposed a feature-based binary classification system using high order statistics to detect image composition [12]. Bayram *et al.*, framed the image forgery detection problem as a feature and classification fusion problem. The authors develop single weak “experts” to detect each image processing operations such as scaling, rotation, contrast shift, and smoothing, among others [13]. Thereafter, these weak classifiers are fused. Chen *et al.*, used inconsistencies in the photo-response non-uniformity noise to detect traces of tampering [5]. When splicing two images to create a composite, one often needs to re-sample

an image onto a new sampling lattice using an interpolation technique (such as bi-cubic). Although imperceptible, the re-sampling contains specific correlations that, when detected, may represent evidence of tampering. Popescu and Farid described the form of these correlations, and proposed an algorithm for detecting them in an image [4]. These image forgery detection approaches are mainly based on general low-level visual features.

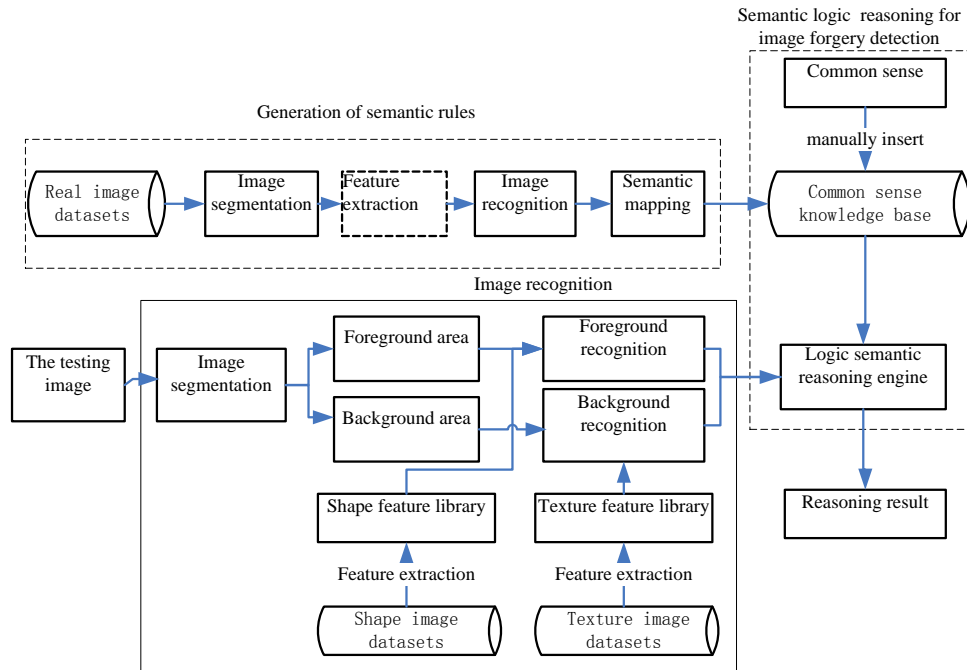
At present, there are many researches on semantic ontology knowledge representation and semantic logic reasoning. Quanrui Wang proposed a semantic reasoning model based on rough logic [14]. The reasoning model is based on the fuzzy set  $M = (U, R)$ , where  $M$  is a fuzzy space,  $U$  represents object in fuzzy space,  $R$  is the relationship between attributes of each object, and has five rough logical values: truth, falsity, rough truth, rough falsity and rough inconsistency. Based on these fuzzy logic values of the fuzzy logic formulas, the authors also give the mathematical proof for the proposed fuzzy logic semantic reasoning model. Manel Kolli introduced the formal rules based on the techniques of description logics to solve the problem of ontology matching process which consists of detecting the semantic mappings between two given ontology [15]. The paper use mathematical language to describe the “problems” and “solutions”, and then put forward five kinds of mapping rules. Last, the correctness of the proposed mapping rules is verified using protégé software. Frank van Harmelen proposed an approximate reasoning method for the semantic web based on the OWL language grammar, semantics, *etc.* [16]. Anni-Yasmin Turhan proposed ontology description logic for semantic web based on main reasoning form of OWL language, namely Description Logic (DLs) [17]. These description logics use structured approaches to describe ontology, and then reason the unknown knowledge based on DLs using ontology and the relationship between ontology and attribute of ontology. Huailin Dong presented the semantic description and logical proof of transforming ER model to the OWL ontology knowledge base using description logic [18]. The above methods are mainly concerned about the knowledge description of ontology and reasoning model based on the knowledge description. Generally, they put forward the reasoning model and give the mathematical verification, or put forward the design prototype and the prototype realization for specific content.

There is little attention on image forgery detection using semantic content of image. Sangwon Lee *et al.*, presented a complete workflow for finding the anomalies within images by combining the methods known in computer graphics and artificial intelligence [9]. They first find perceptually meaningful regions using an image segmentation technique and classify these regions based on image statistics, and then use AI common-sense reasoning techniques to find ambiguities and anomalies within an image as well as perform reasoning across a corpus of images to identify a semantically based candidate list of potential fraudulent images.

### **3. The Proposed Framework of Image Forgery Detection Based on Semantic**

The framework of image forgery detection based on semantic, shown in Figure 1, is divided into three modules: image recognition, generation of semantic rule and semantic logic reasoning for image forgery detection. Firstly, the common sense knowledge base is constructed from real image dataset using generation of semantic rule. Secondly, the object

and background are recognized from testing image using image recognition. Last, image forgery detection is completed based on semantic rule, commonsense knowledge base and result of image recognition from testing image.



**Figure 1. The framework of image forgery detection based on semantic**

### 3.1. Image Recognition

Image recognition is completed through three steps including image segmentation, feature extraction and recognition, resulting in foreground objects and background. An image recognition method based on shape feature and texture feature is used in this paper. This method extracts different features for foreground object and background [19].

The extracted features are matched with the corresponding established feature library. According to matching results, we can identify the objects in the image.

In order to recognize objects in complex images, firstly, the testing image is segmented to two meaningful regions, named foreground regions and background regions. Some pixels are manually annotated. Based on these annotated pixels, the testing image can be automatically divided into foreground regions and background regions. Secondly, the features of foreground regions and background regions are separately extracted as texture feature for background regions and shape feature for foreground regions. The four features including contrast, roughness, linearity and directionality of gray level co-occurrence matrix (GLCM) are computed as texture feature for background regions, and the seven HU invariant moments are selected as the shape descriptors for foreground regions.

Before recognizing image, the texture matching library and shape matching library need to be established firstly. The shape features extracted from MPEG library are considered as shape matching library, and the texture features extracted from texture images (texture image includes BRODATZ library and other image downloaded from Internet) are considered as texture matching library.

After establishing the shape matching library and the texture matching library, the next work is to recognize testing image. Because Mahalanobis distance can be used to effectively calculate the similarity of two unknown samples, Mahalanobis distance is used to recognize image [20]. Mahalanobis distance between sample  $i$  and sample  $j$  is as following:

$$D_{i,j} = \sqrt{(x_i - x_j)^T S^{-1} (x_i - x_j)} \quad (1)$$

Where  $x_i$  and  $x_j$  is a vector consist of  $m$  attributes.  $S$  is sample's covariance matrix.

### 3.2. Image Forgery Detection Based on Semantic Logic Reasoning Model

After obtaining results of image recognition from image recognition module, in order to obtain image semantic information and further implement image forgery detection based on these image semantic, the common sense knowledge base and logic semantic reasoning rules need to be constructed. Thus, there are some problems need to be considered as follows.

1. The representation method for structure of common sense knowledge base. That is, knowledge representation for semantic ontology of the image.

2. The semantic rule. Image semantics consists of objects of image including foreground and background, and the relationship between objects in space and behavior in real life. Therefore, there need an appropriate description logic to describe information contained in the image. Based on this knowledge representation and description logic of semantic ontology, image forgery detection will be conducted during the stage of logic reasoning.

3. The construction of common sense knowledge base for logic reasoning. The common sense knowledge base is composed of common sense information in daily life. There are two implementations. An easy way is an artificial given way. That is, common sense knowledge base is constructed by manual adding according to common sense in daily life. We use this easy way as an attempt to image forgery detection based on semantics. Another way is an automated method based on generation module of semantic rule described in Section 3.3, which has been partly investigated and will be further researched in our future work and be presented in another paper in the future.

4. The construction of the logic reasoning engine based on image high-level semantic. Through the establishment of semantic reasoning engine, image forgery detection is completed by judging whether the testing image semantics is consistent with common sense in common sense knowledge base.

A new fuzzy logic semantic reasoning model for image forgery detection based on high-level semantic of the image is proposed in detail in Section 4. Six kinds of semantic reasoning rules based on fuzzy logic are designed for image forgery detection in our reasoning model, which can give the deterministic and uncertainty reasoning results. Our reasoning model is implemented using protégé software based on OWL language.

### 3.3. Generation of Semantic Rule

The main work of this module is to extract semantic information from real image datasets, and establish the common sense rule between foreground objects, and between foreground object and background object. Firstly, Image segmentation for each image in real image dataset is finished. The proposed image segmentation method, such as image segmentation based on region and image segmentation based on cluster etc, can be used. Secondly, the

ontology in the image is recognized using the proposed image recognition methods, such as template matching image recognition. Last, High-level semantic is extracted based on data mining according to logic relationship between objects in image dataset. The ontology and its relationship are stored using knowledge representation method as common sense knowledge base.

#### 4. Semantic Logic Reasoning Model for Image Forgery Detection

Similar to other semantic reasoning researches, this paper is also based on the entity set  $U$  and the relationship  $R$  between the entities, where  $R$  is implemented based on entity attribute  $P$ .  $x$  represents a concrete object,  $P$  represents ontology properties and  $R$  represents the relationship between the ontology in this paper. Logic representation of semantic reasoning is all possible combinations between entity  $U$ , attribute  $P$  and operation  $R$  of attributes, defined as follows:

(1) Entity Set ( $U$ ):  $x_1, x_2, x_3...$  are the entity which has the same attribute.  $U$  is a set of  $x$ , namely

$$U = U(x)$$

(2) Logic Relation Set ( $R$ ):  $R$  is a result set of interaction between many entities  $U$  and relation  $R$ .

$$U1(x1) \cap U2(x2) \in \forall x1, x2 R(x1, x2)$$

Operation symbol of  $R$  include:

$$\sim, \wedge, \vee, \rightarrow$$

(3) Attribute Set ( $P$ ): Attribute  $P$  is based on the entity set  $U$ . Semantic reasoning is implemented based on attributes  $P$  of each entity  $U(x)$  and reasoning rules. Reasoning rules are the function mapping entity  $U(x)$  to result field:

$$\forall x, y (R(P(x), P(y)) \rightarrow Result)$$

where the *Result* is reasoning result.

##### 4.1. Semantic Reasoning Rule

Based on the five kinds of fuzzy logic values proposed by Quanrui Wang [14], six kinds of semantic reasoning rules are designed for image forgery detection in this paper, including often come up with, may be found with, cannot be found with, often come up in, may be found in, cannot be found, shown as following:

**Sentence 1:** O1 often come up with O2

Has Location

O1, O2

**Sentence 2:** O1 often be found in P1

Has Place1

O1, P1

**Sentence 3:** O1 can be found in P1

Has Place1

O1, P1

**Sentence 4:** O1 cannot be found in P1

Has Place1

O1, P1

**Sentence 5:** P1 cannot be found with P2

Has Place1, Place2

P1, P2

**Sentence 6:** P1 can be found with P2

Has Place1, Place2

P1, P2

Where the O1 and O2 are the ontology in image, and the P1 and P2 are the background of the ontology. Sentence 1, 2, 4 and sentence 5 are deterministic decision rules. Sentence 3 and sentence 6 are uncertainty decision rules. Because the sentence 3 and sentence 6 are the judgment of possibility, the results according to the two sentences are reference results. Image splicing detection is completed using logic reasoning according to the relationship between the ontology (sentence 1), or the relationship between the ontology and background of ontology (sentence 2, sentence 3, sentence 4), or the relationship between the background of the ontology (sentence 5, sentence 6). In other words, the problem of image forgery detection is transformed to prediction of correlation between object 1 (background 1) and object 2 (background 2) by searching appreciate sentence after extracting object from image.

The specific interpretation of the six kinds of rules is presented as following:

**Sentence 1:** object 1 and object 2 are often associated appear.

For example, butterflies often fly around the flowers or stay on the flowers. Therefore, the butterflies and flowers is often associated appear. Here, the butterfly is object 1 and the flower is object 2.

**Sentence 2:** object 1 often appears in place 1.

For example, the swan often swims on the water or lake, so the swan will often appear with water together. That is to say, "the swan appeared in the water" is an authenticity scene. Here, the swan is object 1 and the water is background 1 (or namely place 1).

**Sentence 3:** object 1 may appear in place 1.

For example, the ship will go or stay on the water under the ordinary circumstances. However, the ship sometimes can also be stranded on the shore of lake or sea in some actual cases. So, if a ship appears on the shore nearby lake or sea in an image, we also may think that this scene has certain authenticity and need to be further confirmed, and belongs to sentence 3 where the ship is object 1 and the lake is place 1. If we find a ship stay on the desert, where there is no lake or water nearby, we think that the scene is not true and belongs to sentence 4.

**Sentence 4:** object 1 can't appear in place 1.

For example, the plane will appear on the runway or in the sky under the ordinary circumstances. If it is found that the plane appeared in other places, such as the grass, it is indicated that the image is likely to be forged, where the plane belongs to object 1, and the grass or the desert is place 1.

**Sentence 5:** the background 1(or the place 1) can't appear with the background 2(or the place 2) together.

For example, fire and water are two incompatible objects. Therefore, if water and fire appear together at the same time in an image, we may think that the image is most likely fake image. Here, the water in the image is background 1 and the fire is background 2.

**Sentence 6:** the background 1 and the background 2 often appear together.

For example, as we know, any objects or places are under the sky. Namely, these images are most likely true, such as the desert can appear under the sky, the snow mountain can appear under the sky, and the sea can also appear under the sky.

## 4.2. Ontology Storage Structure

In order to realize the above semantic reasoning rules, we need to build semantic ontology. The storage structure of the ontology and surroundings of ontology in database are designed as follows:

NODE: ontology name (or name of ontology's surroundings)

EDGE1:

PRO: has Property 1

Class: P (or O)

SENTENCE: sentence 1, 2, 3, 4, 5 and 6

DIRECTION: descriptor

EDGE2:

PRO: has Property 2

Class: P (or O)

SENTENCE: sentence 1, 2, 3, 4, 5 and 6

DIRECTION: descriptor

...

Where NODE represents the ontology or ontology's surroundings, PRO represents attributes of object, namely specific attributes which distinguish one ontology from other ontologies, O represents ontology, P represents the ontology's environment, SENTENCE represents the appreciate sentences for ontology, DIRECTION is a descriptor of object, namely unique ID of each object in the OWL language.

## 5. Experimental Procedure and Results

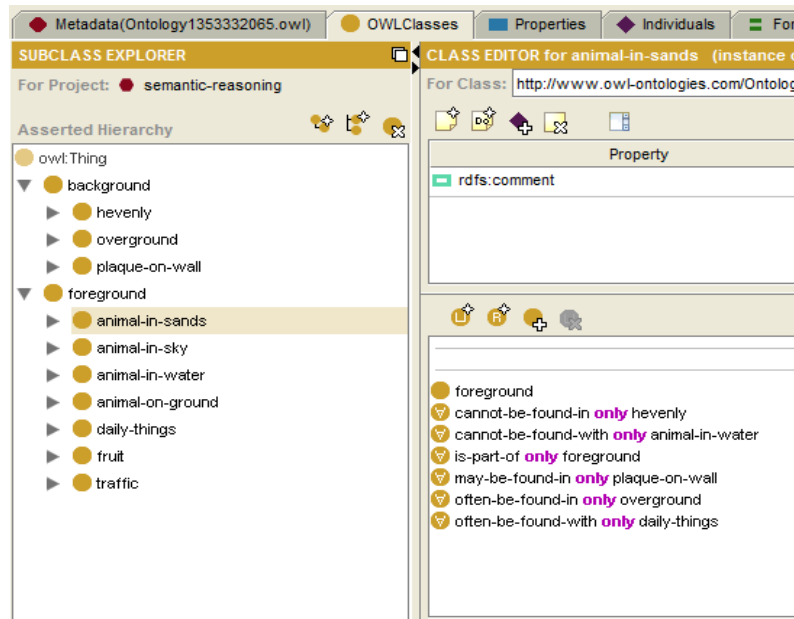
### 5.1. Experimental Environment and Procedure

The experiments in this paper are based on MATLAB 7.8.0, MySQL 5.6.5 database software and ontology software protégé 3.4.3. The ontology and relationship information of ontology are described using the OWL language [21], which is mainly used for the description of the problem of semantic based on description logic. MATLAB is used for image processing and data operation, connection with MySQL database and information query. Protégé is mainly used for construction of ontology including the ontology and semantic relationship between ontology. MySQL database is mainly used to store protégé ontology information and semantic relationship based on the OWL language.

During the experiments, after establishing a connection with MATLAB, MySQL and Protégé software, ontology base is firstly constructed using protégé software. Then, these

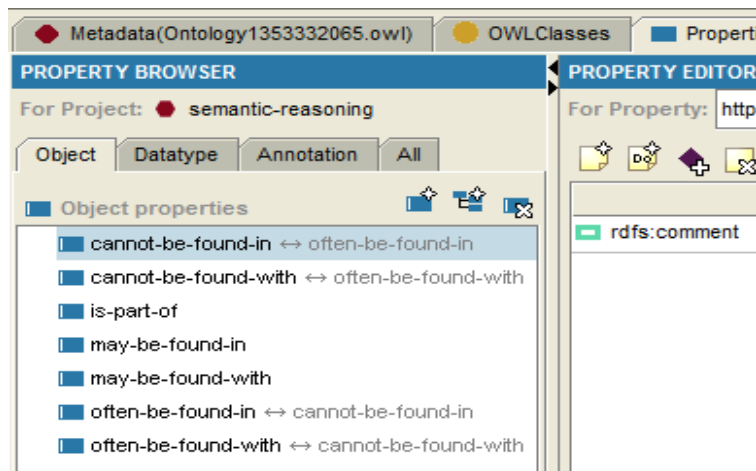


ontologies and its relationship information, called common sense knowledge base, are stored in MySQL database. The foreground objects and background objects of a testing image are recognized based on image recognition method using multi-features [19]. Image forgery detection is completed by inquiring the semantic knowledge base according to the fuzzy logic reasoning rules and operation. The construction procedure of ontology and relationship between ontology in protégé is shown in Figure 2.

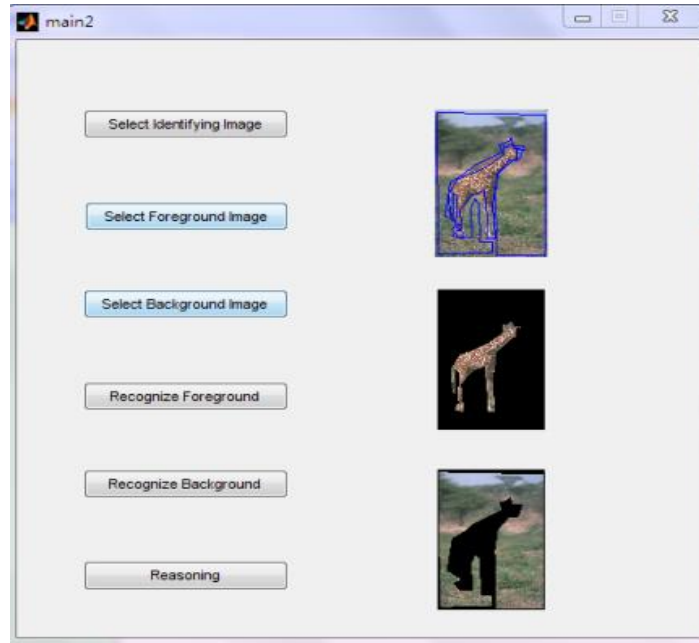


**Figure 2. Ontology and relationship between ontologies with protégé 3.4.3**

Seven kinds of attributes of relationship between ontology are shown in Figure 3. GUI interface is completed using Matlab to show experimental result as shown in Figure 4.



**Figure 3. Properties of ontology and relationship between ontologies with protégé 3.4.3**



**Figure 4. GUI interface of prototype system of image forgery detection based on semantic**

**5.2 Detection Results and Discussion**

The testing images are downloaded from Berkeley segmentation dataset and benchmark [22]. MATLAB will show the corresponding reasoning results after selecting the suitable sentence rules according to the recognition object in an image. Some reasoning results are presented as follows:

**Sentence 1:** O1 often come up with O2.

|  |  |
|--|--|
|  | <pre>Link database of semantic ontology..... msg = The foreground object isbutterfly msg = The foreground object isflower butterfly often-be-found-with flower Link database of semantic ontology.....</pre> |
|  | <pre>msg = The foreground object ispeople msg = The foreground object isboat people often-be-found-with boat</pre>   |

(a) Testing image                      (b) Reasoning result

**Figure 5. Detection results for sentence 1**

**Sentence 2:** object 1 often appears in place 1.



```
Link database of semantic ontology.....  
msg =  
The foreground object ischopper  
msg =  
The background object issky  
chopper often-be-found-in sky
```

(a) Testing image (b) Reasoning result

**Figure 6. Detection results for sentence 2**

**Sentence 3:** object 1 may appear in the place 1.



```
Link database of semantic ontology.....  
msg =  
The foreground object isboat  
msg =  
The background object iswater  
boat may-be-found-in water
```

(a) Testing image (b) Reasoning result

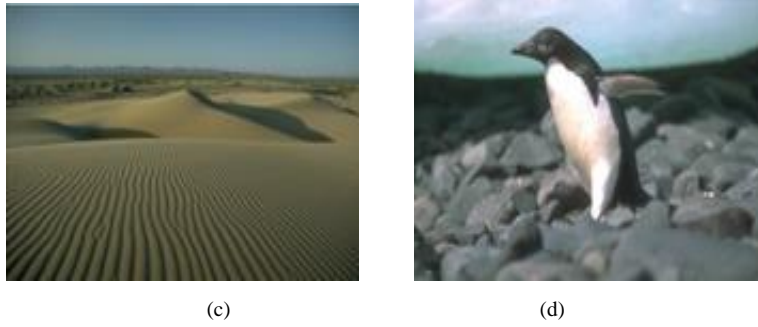
**Figure 7. Detection results for sentence 3**

**Sentence 4:** object 1 can't appear in place 1.



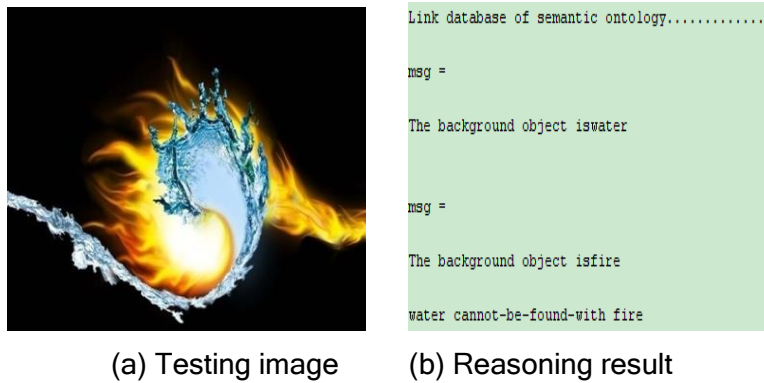
```
Link database of semantic ontology.....  
msg =  
The foreground object ispenguin  
msg =  
The background object iscement  
penguin cannot-be-found-in cement
```

(a) Testing image (splicing image composite of c and d) (b) Reasoning result



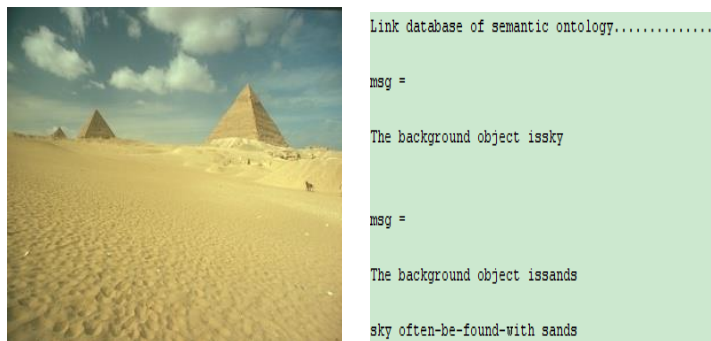
**Figure 8. Detection results for sentence 4**

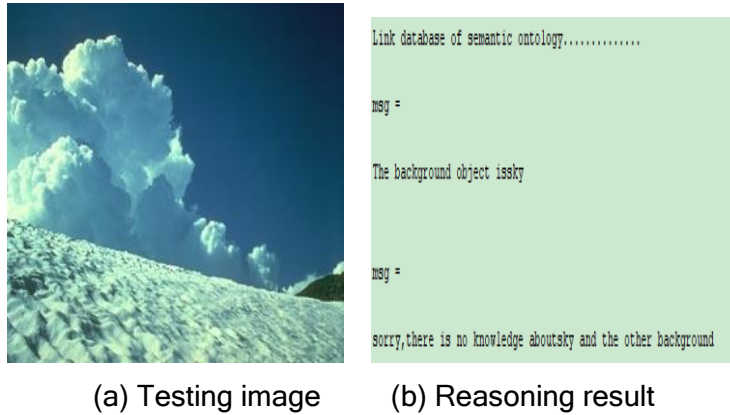
**Sentence 5:** the background object 1(or the place 1) impossible appear with the background objects 2(or the place 1) together.



**Figure 9. Detection results for Sentence 5**

**Sentence 6:** the background object 1 and the background objects 2 often appear together.





**Figure 10. Detection results for Sentence 6**

In the experiments, we tested 500 images obtained from Berkeley image dataset [22] and Columbia Image Splicing Detection Evaluation Dataset [23]. The tampering images are spliced from the foreground and background. The experimental results show that object recognition rate based on image recognition method using multi-features [19] is 83.97%, and the accuracy of the proposed image forgery detection based on semantic logic reasoning model can reach 70.51% on the basis of the correct identification of object in image.

There are two reasons for low detection accuracy. Firstly, the semantic logic reasoning is based on the result of image recognition. If objects in image could not be identified, reasoning could not be completed. Image recognition accuracy is not high enough in our experiments and will be improved in the future work. Secondly, because of manually adding ontology and logic reasoning rule to knowledge base, the common sense knowledge base is not perfect enough, and refinement of logic reasoning rule is not enough. These shortcomings will be further improved in the later research.

## 6. Conclusions and Future Work

This paper discussed the forgery detection problem of digital image from the point of high-level semantic, and proposed the framework of image forgery detection based on semantic and semantic logic reasoning model. The framework consists of three components including image recognition, semantic logic reasoning engine and generation of semantic rule. The result of image recognition for the testing image is used as input of semantic logic reasoning engine. Based on the common sense knowledge base conducted from the module of generation of semantic rule, image forgery detection is completed using semantic reasoning rule of semantic logic reasoning engine. The prototype system of image forgery detection is completed using MATLAB, MySQL database software and ontology software protégé. Although the semantic reasoning rules are relatively simple, semantic knowledge base still need to manually built and the splicing detection rate is relatively low, experimental results show that the framework and logic semantic reasoning model for image forgery detection are feasible.

Because image forgery detection based on image semantic is completed by artificial intelligent, expert system, common sense reasoning, and machine learning technologies from the perspective of simulating human thought, namely from image content and semantic information, avoiding detection using the traditional methods based on low-level image features, it is a very important research approach for image forgery detection. However, the framework is still at the research stage of an experimental prototype. In the future, the

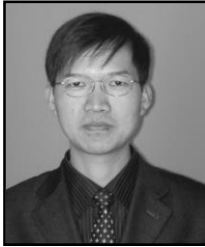
following aspects need to be improved: a) improving semantic reasoning rules to make it richer, more comprehensive and complete to cover as many relations and scenarios in real images as possible; b) improving the image recognition accuracy; c) research on automatic construction of common sense knowledge base extracted from real image dataset based on the proposed semantic image annotation and retrieval methods.

## References

- [1] A. Rocha, W. Scheirer, T. and S. Goldenstein, "Vision of the Unseen Current Trends and Challenges in Digital Image and Video Forensics", *ACM Computing Surveys*, vol. 43, no. 4, (2011), pp. 26:1-26:42.
- [2] F. Hany, "Exposing Digital Forgeries in Scientific Images", *Proceeding of the 8th ACM Workshop on Multimedia and Security*, (2006), pp. 29-36.
- [3] Y. Q. Shi, C. Chen and W. Chen, "A Natural Image Model Approach to Splicing Detection", *Proceeding of the 9th ACM Workshop on Multimedia and Security*, Dallas, TX, United states, (2007), pp. 51-62.
- [4] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling", *IEEE Transactions on Signal Processing*, vol. 53, no. 2, (2005), pp. 758-767.
- [5] M. Chen, J. Fridrich, J. Lukas and M. Goljan, "Imaging Sensor Noise as Digital X-ray for Revealing Forgeries", *Proceeding of the 9th International Workshop on Information Hiding*, (2008), pp. 342-58.
- [6] M. K. Johnson and H. Farid, "Exposing Digital Forgeries in Complex Lighting Environments", *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, (2007), pp. 450-461.
- [7] H. R. Chennamma and L. Rangarajan, "Image Splicing Detection Using Inherent Lens Radial Distortion", *International Journal of Computer Science Issues*, vol. 7, no. 6, (2010), pp. 149-158.
- [8] J. He, Z. Lin, L. Wang and X. Tang, "Detecting Doctored JPEG Images via DCT Coefficient Analysis", *Proceeding of the European Conference on Computer Vision*, (2006), pp. 423-435.
- [9] S. Lee, D. A. Shamma and B. Gooch, "Detecting False Captioning using Common-Sense Reasoning", *Digital Investigation*, vol. 3, no. 1, (2006), pp. 65-70.
- [10] J. Fridrich, D. Soukal and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", *Proceeding of the Digital Forensic Research Workshop*, (2003).
- [11] M. K. Johnson and H. Farid, "Exposing Digital Forgeries through Specular Highlights on the Eye", *Proceeding of the 9th International Workshop on Information Hiding*, Saint Malo, France, (2007), pp. 311-325.
- [12] T. -T. Ng and S. -F. Chang, "Blind Detection of Photomontage using Higher Order Statistics", *Proceeding of the 2004 IEEE International Symposium on Circuits and Systems*, Vancouver, BC, Canada, (2004), pp. V-688-V-691.
- [13] S. Bayram, I. Avcibas, B. Sankur and N. Memon, "Image Manipulation Detection", *Journal of Electronic Imaging*, vol. 15, no. 4, (2006).
- [14] Q. -R. Wang, X. -Y. Li, J. -X. Sun and H. -Y. Feng, "The Model of Semantic Reasoning Based on Rough Logic", *Proceeding of the International Conference on Optics, Photonics and Energy Engineering*, (2010), pp. 269-272.
- [15] M. Kolli and Z. Boufaida, "Composing Semantic Relations among Ontologies with a Description Logics", *Information Technology Journal*, vol. 10, no. 6, (2011), pp. 1106-1112.
- [16] F. Van Harmelen, P. Hitzler and H. Wache, "Approximate Reasoning for the Semantic Web", *Proceeding of the Advanced Course at ESSLLI 2006*, Malaga, Spain, (2006).
- [17] A. -Y. Turhan, "Description Logic Reasoning for Semantic Web Ontologies", *Proceeding of the 1st International Conference on Web Intelligence, Mining and Semantics*, Sogndal, Norway, (2011), pp. 6.
- [18] H. Dong, J. Sun and Q. Wu, "The Semantic Description and Logical Proof on ER Diagram Based on the OWL Language", *Proceeding of the 5th International Conference on Computer Science & Education*, Hefei, China, (2010), pp. 1813-1815.
- [19] Y. Ke and J. Shang, "An Image Recognition Method Using Multi- features", *Proceeding of 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, (2012), pp. 419-423.
- [20] X. Zhang, "Mahalanobis Distance Metric Based Laplacian Mapping for Image Recognition", *Proceeding of the 5th International Conference on Internet Computing for Science and Engineering*, Harbin, Hei Long Jiang, China, (2011), pp. 1-5.
- [21] I. Horrocks, P. F. Patel-schneider, D. L. McGuinness and C. A. Welty, "OWL: a Description Logic Based Ontology Language for the Semantic Web", *The Description Logic Handbook: Theory, Implementation, and Applications (2nd Edition)*, vol. 39, (2007), pp. 249-276.
- [22] Berkeley Segmentation Dataset and Benchmark, <http://www.eecs.berkeley.edu/Research/Projects/CS/vision/bsds/>.

[23] Columbia Image Splicing Detection Evaluation Dataset,  
<http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm>.

## Authors



### Yongzhen Ke

He obtained his BE of computer application at Tianjin Polytechnic University in China in 1997, and received his ME and PhD of computer application at Tianjin University in China in 2000 and 2008, respectively, on the research subjects of information security, image processing and data visualization. From 1997 to the present he worked in Tianjin Polytechnic University, China. Now he is an associate professor at School of Computer Science & Software Engineering, Tianjin Polytechnic University, China. His current research interests include image processing, digital image forensic, network security and application of IoT.



### Weidong Min

He obtained his BE, ME and PhD of computer application at Tsinghua University in China in 1989, 1991 and 1995, respectively, on the research subjects of computer graphics, image processing and computer aided geometric design. He was an assistant professor of Tsinghua University from 1994 to 1995. From 1995 to 1997 he was a postdoctoral researcher at University of Alberta, Canada. From 1998 to 2011 he worked as a senior research project manager at Corel, March Networks and other companies in Canada. Now he is an associate professor at School of Computer Science & Software Engineering, Tianjin Polytechnic University, China. His current research interests include computer graphics, image and video processing, software engineering, distributed system, network resources management.



### Fan Qin

She obtained her bachelor degree of economics at Nankai University in China in 2000, and received her master degree and PhD of management at Nankai University in China in 2005 and 2009, respectively, on the research subjects of information management, data mining. From 2009 to the present she worked in Nankai University, China. Now she is a lecture at department of logistics management, Nankai University, China. Her current research interests include information system management, image recognition, e-commerce and logistics management.



**Junjun Shang**

She obtained her master degree of computer application at Tianjin Polytechnic University in China in 2013. Her current research interests include image processing and digital image forensic.