ISSN:2348-2079

Volume-6 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Ensuring image and text privacy on social networks using CNN and MSER technique

Mrs. Sini. M, IInd Mtech(Applied Electronics and Communication Engg)
Ms. Vandana. P, Assistant Professor, Department of ECE,
Cochin College of Engineering and Technology, Valanchery,
Malappuram Distract, Kerala, India
Mail id: sinimrafi@gmail.com

Abstract

With the glowing popularity of smart-phones and other mobile devices, high-quality cameras are increasingly pervasive. As a result, capturing images and sharing them on social platforms like Facebook, Instagram and Foursquare has become a common part of our daily life. However, without the proper privacy protection, the shared images with or without text can reveal much of users' personal and social environments and their private lives since images can intuitively tell when and where a special moment took place, who participated and what were their relationships. Unfortunately, many people especially young users of social networks often share private images about themselves, their friends and classmates without being aware of the potential impact on their future lives caused by unwanted disclosure and privacy violations. This paper introduces the concept of Maximally Stable Extremal Regions (MSER) and CNN to the privacy settings prevailing. The Convolutional Neural Network (CNN) is employed to protect the sensitive objects in the image. The Maximally Stable Extremal Regions (MSER) is adapted to protect the text regions under the images.

Index Terms: Digital Image Processing, Image privacy, Text privacy, Convolutional Neural Networks (CNN), Multi task learning and Sensitive objects.

1. Introduction

In the past several years, Convolutional Neural Networks have demonstrated exceptional performance on complex visual tasks. They have shown state of the art results on the CIFAR-10, CIFAR- 100, and ImageNet datasets, among others. Unfortunately, the discriminative power of large convnets is also their weakness. They overfit to the training data easily, and are prone to getting stuck in local minima. This problem is less pronounced on large datasets such as Imagenet; and it has been circumvented on some datasets by pre-training using ImageNet and fine-tuning on the final task.

Nevertheless, sometimes either a large and related task is unavailable, or the several days it takes to pre-train on that task is too costly. This leaves the discriminative power provided by convnets impossible to harness. In this paper, we introduce novel ways of regularizing the convnet. We explore different ways of forming related tasks to the original task by agglomerating classes into super-classes, which then can be trained jointly with the original task in a form of multi-task learning. We see significant improvement in generalization performance. Furthermore, we have found that part-way through training, a random re-initialization of later layers in the network also significantly boosts test-time performance.

2. Related Work

Most modern OSNs allow users to control the privacy settings of their shared content. Yet, the typical user finds it difficult to understand and correctly configure the offered access control policies [9]. As a result, several

studies [10] have identified a serious mismatch between the desired and the actual privacy settings of online shared content. This discrepancy motivated the development of mechanisms that aid users in selecting appropriate privacy settings. In the work of [1], for instance, the authors focused on Facebook posts and evaluated prediction models that make use of users' previous posts and profile preferences in order to suggest appropriate privacy settings for new posts. Despite achieving high performance, the authors noticed differences in user behaviors and concluded that personalized privacy models could further improve the results.

Zerr et al. [8], were among the first to consider the problem of privacy-aware image classification. In their work, a large-scale user study was conducted asking participants to annotate a large number of publicly available Flickr photos as being either \private" or \public". The study was set up as a social annotation game where players were instructed to adopt a common definition of privacy7 and were rewarded for providing annotations that were similar to those of other players. The resulting dataset, referred to as PicAlert, was used to train supervised classification models that capture a generic notion of privacy.

Extending that work, experimented with combinations of visual and metadata-derived features and achieved better prediction accuracy on PicAlert. [2] also attempted to solve a more complex privacy classification problem where three types of disclosure were defined for each image and the task was to assign one of five privacy levels to each type of disclosure. Their models captured only a generic perception of privacy.

Differently from the majority of previous works, our paper highlights the limitations of generic image privacy classification models and proposes an effective personalization method. To the best of our knowledge, [4] is the only work that considers privacy classification of personal photos as we do here. However, [4] evaluates only purely personalized models, assuming that each user provides sufficient amount of feedback. In contrast, our method achieves high performance even at the presence of very limited user-specific feedback by leveraging feedback from other users. Moreover, uses only metadata-based and simple visual features, we employ state-of-the-art CNN-based semantic visual features that facilitate comprehensible explanations of the classification outputs. Very recently, [3] evaluated the performance of deep features on PicAlert and found that they yield remarkable improvements in performance compared to SIFT, GIST and user-assigned tag features. Moreover, the authors evaluated the performance of `deep tag' features but did not exploit them for justifying the classifier's decisions.

3. Image Privacy Protection on Social Networks

With the growing popularity of smart-phones and other mobile devices, high-quality cameras are becoming increasingly ubiquitous and pervasive, as a result, capturing high-quality images has become one part of our daily activities and image sharing has now become very popular in social platforms like Facebook, Instagram and Foursquare. By default, the shared images can be seen by anyone in social networks. Since images can intuitively tell when and where a special moment took place, who participated and what were their relationships, the shared images can reveal much of users' personal and social environments and their private lives [5]. Thus, privacy protection is a critical issue to be addressed during social image sharing. Unfortunately, many people especially young users of social networks often share private images about themselves, their friends and classmates without being aware of the potential impact on their future lives caused by unwanted disclosure and privacy violations.

To ensure privacy, most social image sharing sites allow users to manually specify coarse-grained privacy settings: whether an image is public, private or visible to their family members or friends. However, due to the lack of privacy knowledge, it would not be easy for common users to correctly configure privacy settings to achieve their desired levels of privacy protection; also, given the large number of images being shared and the tedious steps needed for fine-grained privacy settings, some users may not be willing to spend extra time on providing such fine-grained privacy settings.

Based on these observations, in this work, a new approach called iPrivacy (image Privacy) is developed to automate such privacy setting process for social image sharing. Unlike many previous works typically recommend privacy settings based on similarity of users' profiles or image tags, our idea is to automatically detect the privacy-sensitive objects from the images being shared, recognize their classes, and identify their privacy settings, so that the image owners can be warned what objects in the images need to be protected before sharing [6]. The critical challenge to be conquered here is how to identify all the privacy-sensitive object classes efficiently and learn the object-privacy relatedness precisely from massive social images, so that such knowledge can later be used to: (1) determine which object classes should be detected from individual images being shared; and (2) leverage object detection results to recommend the best-matching privacy settings for image sharing. Considering 1.82 billions active users of social networks and trillions of shared images, there may exist a large set of privacy-sensitive object classes. Such privacy-sensitive object classes can further be partitioned into two categories: (a) user-independent classes such as humans, locations and discrimination texts in images; and (b) user-dependent classes such as home shrines and visual attributes for personal hobbies.

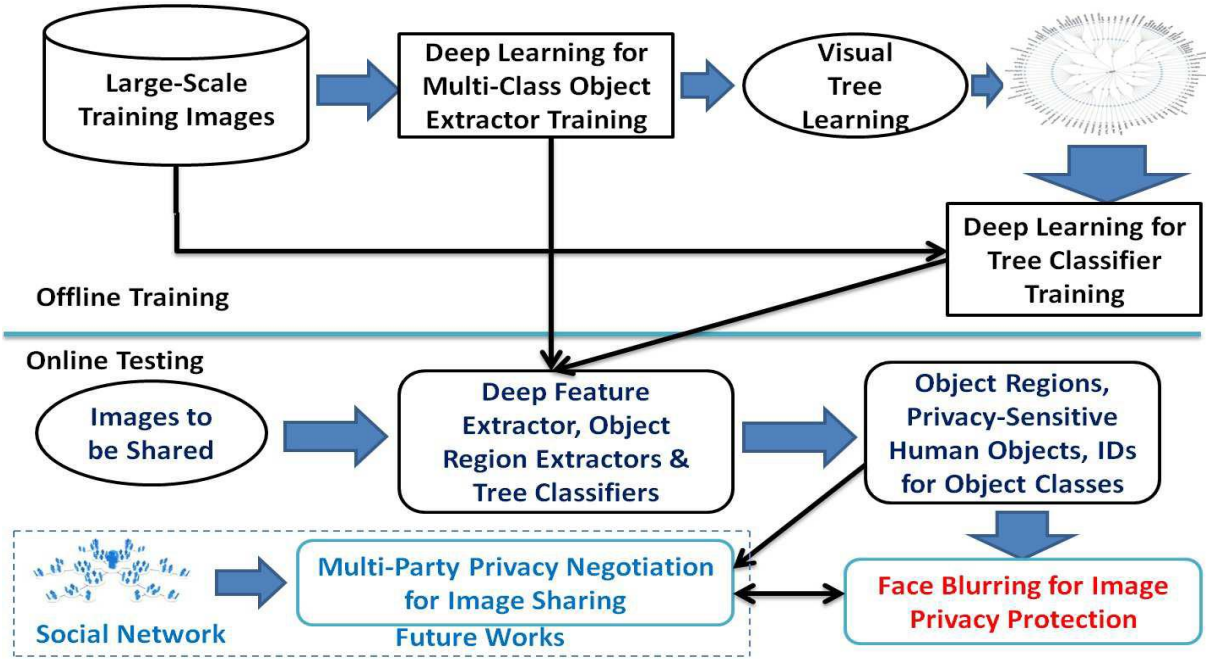

Fig. 1. An Overview of the key components of our iPrivacy system.

Another critical issue for automating the privacy setting process is the time limitation, e.g., users may expect to get their privacy setting recommendations quickly. Because there could have large numbers of privacy-sensitive object classes, detecting the privacy-sensitive objects from the images being shared and recognizing their classes could be very expensive, thus recommending the best-matching privacy settings for image sharing could be an extremely time consuming process. Specifically, if a flat approach is employed, the computational cost will grow linearly with the total number of privacysensitive object classes and hence it is not scalable; if a hierarchical approach is adopted, the object detection process could be speed up dramatically but it would seriously suffer from the so-called inter-level error propagation problem, i.e., the mistakes made at the parent nodes will propagate to their child nodes and such mistakes cannot be recovered.

To address the aforementioned challenges, our iPrivacy system takes four main steps (as illustrated in Fig. 1): (1) Deep CNNs are learned to achieve semantic image segmentation and identify large numbers of object classes from massive social images, and an automatic object-privacy alignment algorithm is developed to learn the object-privacy relatedness and identify a large set of privacy-sensitive object classes; (2) A visual tree is learned to organize large numbers of privacy-sensitive object classes hierarchically in a coarse-to-fine fashion, which can provide a good environment to determine the inter-related learning tasks automatically; (3) A hierarchical deep multitask learning (HD-MTL) algorithm is developed to learn more representative deep CNNs and more discriminative tree classifier jointly over the visual tree, so that we can achieve fast and accurate detection of large numbers of privacy-sensitive object classes; (4) A soft prediction scheme is used to enhance the performance of our hierarchical object detection approach by exploiting multiple paths simultaneously [7]. A simple solution for image privacy protection is further provided by blurring the privacy-sensitive objects automatically. We have conducted extensive experimental studies on real-world images and the results have demonstrated both efficiency and effectiveness of our proposed approach.

4. Problem Statement

Privacy protection during image sharing is still a challenging task. iPrivacy is an automated privacy setting process. Based on hierarchical deep multi task learning algorithm & deep convolutional neural networks. Deep CNN are learned to achieve semantic image segmentation. A visual tree is used to organize large no. of privacy sensitive object classes hierarchically. HD – MTL algorithm is developed. A prediction scheme is used to enhance the performance. Automated image privacy protection by identifying sensitive objects/areas.

5. Joint Learning of Deep CNNS and Tree Classifier for Large-Scale Object Detection

The third step in our iPrivacy system is to learn the tree classifier and the deep CNNs jointly over the visual tree in an end-to-end fashion, so that we can achieve fast and accurate detection of large numbers of privacy-sensitive object classes. Our deep network for hierarchical object detection are partitioned into three parts: (a) 3 commonlyshared convolutional layers learn the common representations for all the privacy-sensitive object classes; (b) 2 group-specific convolutional layers and 2 group-specific fully-connected layers to learn the class-specific representations for the visually similar privacy-sensitive object classes in the same group, e.g., the sibling privacy-sensitive object classes under the same parent node; and (c) the last layer for the tree classifier to replace the flat softmax-layer. Because each group contains only a small number of visually-similar privacy-sensitive object classes, we scale down the number of kernel mappings for the 2 group-specific convolutional layers and 2 fully-connected layers into 10% of that for the deep CNNs in Caffe and Dropout is applied to 2 group-specific fully-connected layers with a value of 0.5 to prevent over-fitting.

A bottom-up approach is further developed to achieve joint learning of the deep CNNs and the tree classifier over the visual tree: (a) To distinguish the visually-similar privacy sensitive object classes at the sibling leaf nodes under the same parent node, a deep multi-task learning algorithm is developed to train their multi-task softmax classifiers jointly for enhancing their discrimination power, and a joint objective function is used to simultaneously refine both the multi-task softmax classifiers for the sibling leaf nodes and the deep CNNs for image representation; (b) A hierarchical deep multi-task learning (HD-MTL) algorithm is developed to train more discriminative classifiers for high-level nodes and control the inter-level error propagation effectively, where a joint objective function is used to simultaneously update both the tree classifier and the deep CNNs.

5.1. Deep Multi-Task Learning

It is worth noting that our visual tree has provided a good environment to identify the inter-related learning tasks automatically, e.g., the tasks for learning the classifiers for the sibling leaf nodes under the same parent node are strongly inter-related because such sibling privacy-sensitive object classes share some

common visual properties significantly. A deep multi-task learning algorithm is developed to train such inter-related classifiers jointly to enhance their discrimination power, where the inter-task relationships are leveraged to regularize the manifold model structures. The complexity for joint classifier training can be controlled effectively by focusing on at most B sibling privacy-sensitive object classes under the same parent node and the negative images can be selected locally from other sibling leaf nodes under the same parent node. For a given parent node ch at the second level of the visual tree, the multi-task softmax classifiers for its visually-similar privacy-sensitive object classes are trained simultaneously by optimizing a joint objective function.

By embedding the inter-class visual similarities into a manifold structure regularization term, our deep multi-task learning algorithm can explicitly consider the differences of the inter-task relationships and their effects on multi-task learning. By focusing on the visually similar privacy-sensitive object classes under the same parent node, our deep multi-task learning algorithm can effectively control the complexity for joint classifier training and achieve good sample balance by selecting the negative instances locally from other visually-similar privacy-sensitive object classes under the same parent node. Our deep multi-task learning algorithm can simultaneously compare and contrast the visually-similar privacy-sensitive object classes to enhance their separability, thus it is able to establish two separable decision functions: (1) the common prediction function shared among the multi-task softmax classifiers for the visually similar privacy-sensitive object classes under the same parent node; and (2) the class-specific prediction function for the multi-task softmax classifier for each privacy-sensitive object class.

By explicitly separating the common prediction function from the class-specific prediction function, our multi-task softmax classifiers can have higher discrimination power on distinguishing the visually-similar privacy-sensitive object classes under the same parent node, e.g., learning such inter-related tasks jointly can reduce the risk of over-fitting to a specific detection task and boost the performance of all the individual detection tasks. Because the visually-similar privacy-sensitive object classes have similar learning difficulty, the gradients of their joint objective function could be more uniform and the back propagation operations can stick on reaching the global optimum effectively.

We jointly learn the multi-task softmax classifiers for multiple visually-similar privacy-sensitive object classes under the same parent node and the deep CNNs according to the joint objective function. The errors of these inter-related learning tasks are back-propagated to update the weights for the deep CNNs. Given a training instance, the predictions of the inter-related tasks are calculated. We formulate the training error rate in the form of softmax regression:

5.2. Hierarchical Deep Multi-Task Learning

One salient principle of our hierarchical object detection approach is that: an image or an object proposal x from the image should first be assigned into the parent node correctly if it can further be assigned into the child node thus an inter-level relationship constraint is defined inter-level relationship constraint can fully capture the correlation of inter-level predictions and its effects on hierarchical classifier training, e.g., it can force our hierarchical deep multi-task learning (HDMTL) algorithm to train more discriminative classifiers for the high-level nodes on the visual tree, so that the tree classifier can control the inter-level error propagation effectively. It is worth noting that distinguishing the coarse-grained groups of privacy-sensitive object classes on the high-level non-leaf nodes is much easier than distinguishing the visually similar privacy-sensitive object classes on the sibling leaf nodes, thus it is possible for us to learn more discriminative classifiers for the high-level non-leaf nodes on the visual tree. Another salient principle of our hierarchical object detection approach is that: all the images or all the object proposals, which can be assigned into the same parent node correctly, should further be able to be assigned into the relevant child nodes, thus an inter-level complementarity constraint.

By leveraging the visual tree to generate subtrees iteratively and determine the inter-related learning tasks automatically, our

hierarchical deep multi-task learning (HDMTL) algorithm can provide an iterative solution for largescale machine learning, so that training large numbers of node classifiers over the visual tree becomes computationally tractable. Such tree classifier can effectively rule out unlikely coarse-grained groups of privacy-sensitive object classes at an early stage, which can significantly reduce the computational cost for detecting and recognizing the privacysensitive objects from the images to be shared. By leveraging two inter-level constraints force our HD-MTL algorithm on training more discriminative classifiers for the high-level non-leaf nodes on the visual tree, our tree classifier can control the inter-level error propagation effectively and obtain high accuracy rates on large-scale object detection.

For the sibling high-level non-leaf nodes on the visual tree, we jointly train: (a) their multi-task softmax classifiers; and (b) the deep CNNs according to the joint objective function. We use back-propagation to update: (1) the multi-task softmax classifiers for the sibling high-level non-leaf nodes under the same parent node; (2) the multi-task softmax classifiers for their child nodes at the lower levels of the visual tree until the relevant leaf nodes; and (3) the weights for the deep CNNs. Given a training image or an object proposal from the training image, predictions of the interrelated tasks are calculated, and the corresponding gradients are back-propagated fine-tune both the tree classifier and the deep CNNs simultaneously.

6. Protecting Image and Text Privacy using CNN and MSER

They are Similar to SIFT detector, Extracts from an image i a number of co-variant regions, called Maximally Stable Extremal Regions (MSERs) and Identify the stable regions. The region is grown by comparing all unallocated neighboring pixels to the region. The difference between a pixel's intensity value and the region's mean, is used as a measure of similarity. This process stops when the intensity difference between region mean and new pixel becomes larger than a certain threshold. Edge detection - finds the boundaries of objects within images works by detecting discontinuities in brightness. Common edge detection algorithms include Sobel, Canny, Prewitt, Roberts, and fussy logic method. The region is grown by comparing all unallocated neighboring pixels to the region. The difference between a pixel's intensity value and the region's mean is used as a measure of similarity. This process stops when the intensity difference between region mean and new pixel becomes larger than a certain threshold. Convolutional Neural Networks for semantic segmentation of object regions. Use conditional random field model image clustering based on semantic similarity. Deep Multi Task Learning used for large scale image classification. Integrates deep CNN multi task learning concept ontology low cost and higher level of accuracy. Not used directly bze of two reasons. They are object classes are organised hierarchically and multiple deep CNN are used to learn about the features of groups and object classes.

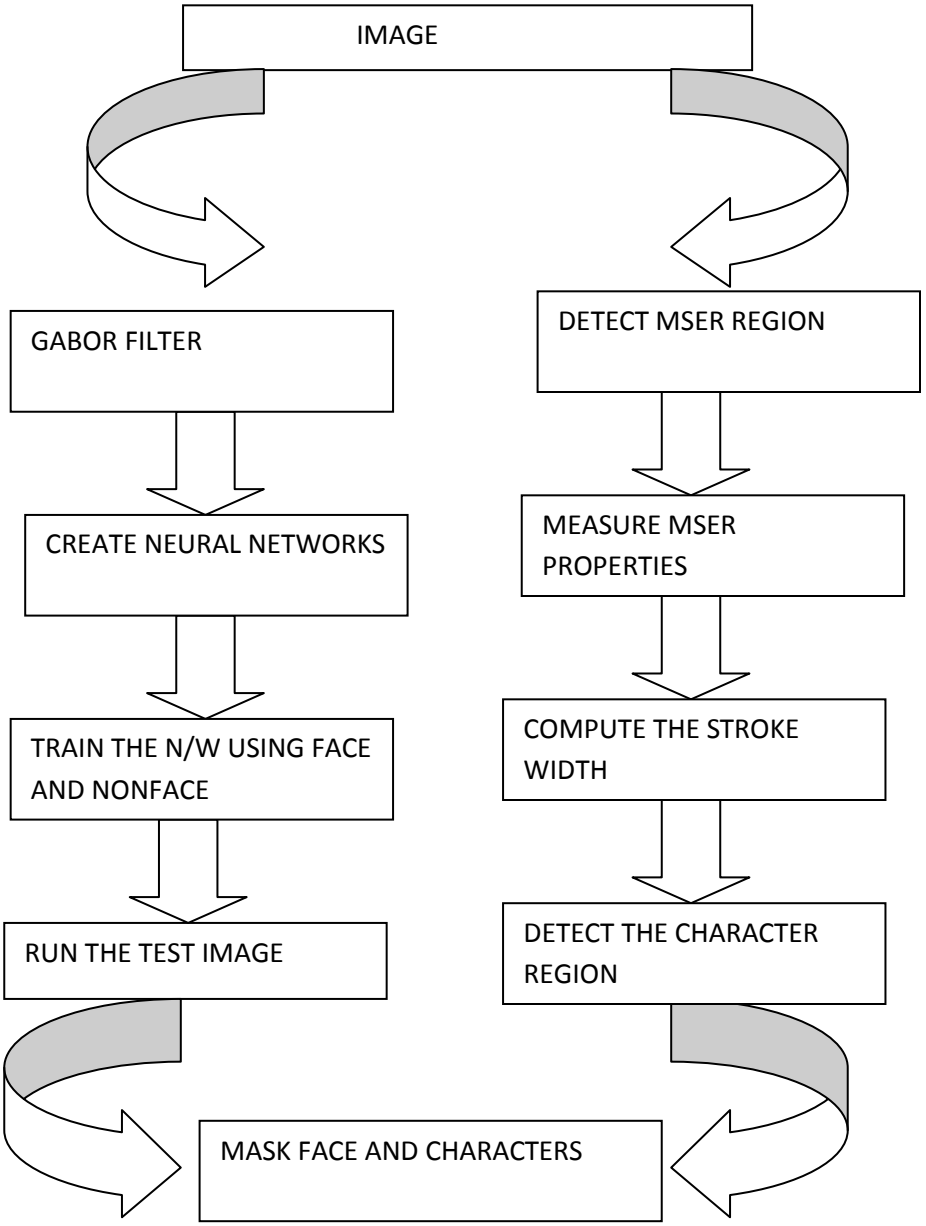

Figure No: 6.1. Block Diagram for Image and Text Privacy Protection

The image and text privacy protection scheme is build with Convolutional Neural Network (CNN) and Maximally Stable Extremal Regions (MSER) techniques. Figure 6.1. shows the block diagram for the text and image privacy protection process. The sensitive objects in the images that are shared through the social networks are protected in the system. The image is passed to the Gabor filter for the feature extraction process. The neural network is constructed with the image features and labels. The face and non faces are used to train the neural networks. The test image running process is called to protect the privacy objects. The faces and characters are massed in the privacy protection process. The Maximally Stable Extremal Regions (MSER) region detection is called to identify the objects and characters regions. The MSER properties are measured for the image. The character stroke width is computed with the measurements. The character region is identified with the character strokes.

The character regions are passed to the masking process.

7. Conclusions and Future Work

To automate image privacy protection, a new approach called iPrivacy is developed in this paper to support privacy setting recommendation for image sharing. By learning the object-privacy relatedness from massive social images, our object-privacy alignment algorithm can allow us to identify a large set of privacy-sensitive object classes and their privacy settings automatically. By learning the deep CNNs and the tree classifier jointly over the visual tree in an end-to-end way, our HD-MTL algorithm can achieve fast and accurate detection of large numbers of privacy-sensitive object classes and recommend the best-matching privacy settings for image sharing. An simple solution for image privacy protection is further provided by automatically blurring the privacy-sensitive objects during the image sharing process. Our experimental results have demonstrated that our HD-MTL algorithm can achieve very competitive results on both the accuracy rates and the computational efficiency. In the future development the image and text privacy protection can be applied on the video files.

REFERENCES

[1] K. D. Naini, I. S. Altingovde, R. Kawase, E. Herder, and C. Nieder_ee. Analyzing and predicting privacy settings in the social web. In User Modeling, Adaptation and Personalization, 2015.

[2] A. C. Squicciarini, C. Caragea, and R. Balakavi. Analyzing images' privacy for the modern web. In In ACM Hypertext, pages 136{147, 2014.

[3] A. Tonge and C. Caragea. Image privacy prediction using deep features. In AAAI Conference on Artificial Intelligence, 2016.

[4] D. Buschek, M. Bader, E. von Zezschwitz, and A. D. Luca. Automatic privacy classification of personal photos. In Human-Computer Interaction - INTERACT, 2015.

[5] Jianping Fan, Zhenzhong Kuang, Baopeng Zhang, Jun Yu, Dan Lin "iPrivacy: Image Privacy Protection by Identifying Sensitive Objects via Deep Multi-Task Learning", IEEE Transactions On Information Forensics And Security, 2016.

[6] Parham M. Kebria1, Saba Al-wais, Hamid Abdi, and Saeid Nahavandi, "Kinematic and Dynamic Modelling of UR5 Manipulator", IEEE International Conference on Systems, Man, and Cybernetics, October 9-12, 2016.

[7] Ehsan Olfat and Mats Bengtsson, "Joint Channel and Clipping Level Estimation for OFDM in IoT-based Networks", IEEE Transactions on Signal Processing, Volume: 65, Issue 18, Sept.15, 2017.

[8] S. Zerr, S. Siersdorfer, J. S. Hare, and E. Demidova. Privacy-aware image classification and search. In ACM SIGIR, 2012.

[9] M. Madejski, M. L. Johnson, and S. M. Bellovin. A study of privacy settings errors in an online social network. In Tenth Annual IEEE International Conference on Pervasive Computing and Communications, 2012.

[10] Y. Liu, P. K. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In Proceedings of the 11th ACM SIGCOMM Internet Measurement Conference, 2011.