Secure Key Generation for Static Visual Watermarking by Machine Learning in Intelligent Systems and Services

Kensuke Naoe, Keio University, Japan
Hideyasu Sasaki, Ritsumeikan University, Japan
Yoshiyasu Takefuji, Keio University, Japan

ABSTRACT

The Service-Oriented Architecture (SOA) demands supportive technologies and new requirements for mobile collaboration across multiple platforms. One of its representative solutions is intelligent information security of enterprise resources for collaboration systems and services. Digital watermarking became a key technology for protecting copyrights. In this article, the authors propose a method of key generation scheme for static visual digital watermarking by using machine learning technology, neural network as its exemplary approach for machine learning method. The proposed method is to provide intelligent mobile collaboration with secure data transactions using machine learning approaches, herein neural network approach as an exemplary technology. First, the proposed method of key generation is to extract certain type of bit patterns in the forms of visual features out of visual objects or data as training data set for machine learning of digital watermark. Second, the proposed method of watermark extraction is processed by presenting visual features of the target visual image into extraction key or herein is a classifier generated in advance by the training approach of machine learning technology. Third, the training approach is to generate the extraction key, which is conditioned to generate watermark signal patterns, only if proper visual features are presented to the classifier. In the proposed method, this classifier which is generated by the machine learning process is used as watermark extraction key. The proposed method is to contribute to secure visual information hiding without losing any detailed data of visual objects or any additional resources of hiding visual objects as molds to embed hidden visual objects. In the experiments, they have shown that our proposed method is robust to high pass filtering and JPEG compression. The proposed method is limited in its applications on the positions of the feature sub-blocks, especially on geometric attacks like shrinking or rotation of the image.

Keywords: Copyright Protection, Digital Watermarking, Key Generation, Machine Learning, Neural Network

DOI: 10.4018/jssoe.2010092103
INTRODUCTION

In this article, we propose a method of key generation scheme (Figure 1) for static visual digital watermarking (Figure 2) by using machine learning technology, neural network as its exemplary approach for machine learning method.

The proposed method is to provide intelligent mobile collaboration with secure data transactions using machine learning approaches, wherein neural network approach as an exemplary technology. First, the proposed method of key generation is to extract certain type of bit patterns in the forms of visual features out of visual objects or data as training data set for machine learning of digital watermark. Second, the proposed method of watermark extraction is processed by presenting visual features of the target visual image into extraction key or herein is a classifier generated in advance by the training approach of machine learning technology. Third, the training approach is to generate the extraction key which is conditioned to generate watermark signal patterns only if proper visual features are presented to the classifier. In our proposed method, this classifier which is generated by the machine learning process is used as watermark extraction key.

The proposed method is to contribute to secure visual digital watermarking without losing any detailed data of visual objects or any additional resources of hiding visual objects as molds to embed hidden visual objects. The proposed method has used neural network for its training approach not limited but open in its applications to other machine learning approaches including fuzzy, Bayesian network and others. In this article, the target content is a static visual data which are constructed with

---

Figure 1. Key generation scheme in embedding procedure

![Figure 1](image-url)

Watermark patterns to be hidden

3) Watermark patterns are presented to classifier as training data set

Target content for copyright protection

2) Feature Extraction performed according to the values of feature extraction key

classifier

4) Extracted features are presented to the classifier as input pattern set

feature extraction key

1) Feature extraction attributes (Coordinate, regions of frequency coefficients selection) saved as feature extraction key

Watermark extraction key

5) Machine learning is processed so that the classifier output watermark when input patterns are presented

6) Converged classifier saved as watermark extraction key
Designing Secure and Privacy-Aware Information Systems
www.igi-global.com/article/designing-secure-and-privacy-aware-information-systems/190419?camid=4v1a

Open Innovation: Assessing the Socio-Economic Factors of Global Software Development
www.igi-global.com/chapter/open-innovation/117292?camid=4v1a

An Emotional Scene Retrieval Framework for Lifelog Videos Using Ensemble Clustering
www.igi-global.com/article/an-emotional-scene-retrieval-framework-for-lifelog-videos-using-ensemble-clustering/126612?camid=4v1a