Information Hiding by Machine Learning: A Method of Key Generation for Information Extracting Using Neural Network

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

ABSTRACT

In this paper, the authors propose information hiding by machine learning: a method of key generation for information extracting using neural network. The method consists of three layers for information hiding. First, the proposed method prepares feature extraction keys, which are saved by feature extraction attributes like feature coordinates and the region of frequency coefficients. Second, the proposed method prepares hidden patterns in advance to the embedding procedure as a watermark signal of the target contents. Finally, the proposed method generates information extraction keys by using machine learning to output presented hidden patterns. The proper hidden patterns are generated with the proper information extraction key and feature extraction key. In the experiments, the authors show that the proposed method is robust to high pass filtering and JPEG compression. The proposed method contributes to secure visual information hiding without damaging any detailed data of the target content.

Keywords: Digital Watermarking, Feature Extraction, Image Authentication, Information Hiding, Key Generation, Neural Network

INTRODUCTION

In this paper, we propose a method of key generation scheme for static visual information hiding by using machine learning technology, neural network as its exemplary approach for machine learning method.

The proposed method is to hide bit patterns as training data set for machine learning and the generated classifier acts as an information extraction key. These hidden patterns are prepared in advance to embedding procedure for the purpose of fingerprint or watermark signal of the target content. Machine learning is processed so that the generated classifier herein is neural network, to output the presented hidden patterns when feature values are presented to the classifier. This feature values are extracted using feature extraction key which is prepared before the embedding process. Feature extraction key

DOI: 10.4018/joci.2011010102
contains information such as feature coordinates and regions of frequency coefficients. Also, the generated classifier in the machine learning process is saved as information extraction key for extraction process. Information extraction procedure is properly processed only by having two proper keys of feature extraction key and information hiding key.

Our method consists of three layers for digital watermarking as an application of our information hiding and information retrieval method: The first layer prepares feature extraction key, which is saved by feature extraction attributes including feature coordinates and regions of frequency coefficient of visual information; The second layer prepares watermark bit patterns to be related with the target content, in advance to the third embedding procedure, as watermark values of the visual information; And, the third layer generates watermark extraction key which is the classifier generated by the machine learning process. The discussed watermark extraction key and feature extraction key identify the related or associated hidden pattern which is the watermark values for proper digital watermarking procedure as shown in Figures 1 and 2.

The proposed method is to contribute to secure visual information hiding without losing any detailed data of 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 paper, the target content is a static visual data which are constructed with discrete data set and we have demonstrated the feasibility of solving this problem by using neural network model. We would enhance our method by using those other approaches, such as fuzzy for dynamic visual data like video stream data and Bayesian network for continuous data structures. This paper is different from the previous work by Ando and Takefuji (2003) in terms of embedding size where this paper does not embed any information to the target content and also implies

**Figure 1. Key generation scheme in the proposed method**
Particle Swarm Optimization Algorithm in Electromagnetics- Case Studies: Reconfigurable Radiators and Cancer Detection
[www.igi-global.com/chapter/particle-swarm-optimization-algorithm-electromagnetics/72824?camid=4v1a](www.igi-global.com/chapter/particle-swarm-optimization-algorithm-electromagnetics/72824?camid=4v1a)

From Swarm Art Toward Ecosystem Art
[www.igi-global.com/article/swarm-art-toward-ecosystem-art/70744?camid=4v1a](www.igi-global.com/article/swarm-art-toward-ecosystem-art/70744?camid=4v1a)