European Research in Telemedicine/La Recherche Européenne en Télémédecine (2017) xxx, xxx—xxx

Available online at ScienceDirect www.sciencedirect.com

Elsevier Masson France EM|consulte www.em-consulte.com/en

ORIGINAL ARTICLE /*Remote Consultation*

Steganalysis via a convolutional neural network using large convolution filters for embedding process with same stego key: A deep learning approach for telemedicine

Stéganalyse via un réseau de neurones convolutionnel à partir de larges filtres de convolution, pour des embarquements utilisant une seule clé : une approche deep learning *pour la télémédecine*

M. Salomon, R. Couturier, C. Guyeux*, J.-F. Couchot, J.M. Bahi

Femto-ST Institute, UMR 6174 CNRS, University of Bourgogne Franche-Comté, 16, route de Gray, 25000 Besançon, France

Received 30 April 2017; accepted 3 June 2017

KEYWORDS
Telemedicine security;
Steganography;
Steganalyzis;
Deep learning

Summary
Introduction. — Steganography, the art to hide information inside host media like pictures and movies, and steganalysis, its countermeasure attempting to detect the presence of an hidden information within an innocent-looking document, are frequently reported as promising information security techniques for telemedicine. For the past few years, in the race between image steganography and steganalysis, deep learning has emerged as a very promising alternative to steganalyzer approaches based on rich image models combined with ensemble classifiers. A key knowledge of image steganalyzer, which combines relevant image features and innovative classification procedures, can be deduced by a deep learning approach called convolutional neural networks (CNN). This kind of deep learning networks is so well-suited for classification tasks based on the detection of variations in 2D shapes that it is the state-of-the-art in many image recognition problems.
Materials and methods. — We design a CNN-based steganalyzer for images obtained by applying steganography with a unique embedding key. The proposed CNN has a quite different shape compared to the ones resulting from the earlier works, and it is able to provide high detection accuracy for several steganographics tools when the same stego key is reused during the

* Corresponding author.
E-mail address: christophe.guyeux@univ-fcomte.fr (C. Guyeux).

http://dx.doi.org/10.1016/j.eurtel.2017.06.001

Please cite this article in press as: Salomon M, et al. Steganalysis via a convolutional neural network using large convolution filters for embedding process with same stego key: A deep learning approach for telemedicine. Eur Res Telemed (2017), http://dx.doi.org/10.1016/j.eurtel.2017.06.001

embedding process. The convolutional part of our proposal starts by a global filtering, using a single filter, followed by a second convolutional layer that produces a reduced set of high-level features (256 features for 512 × 512 pixels input images) thanks to the use of large filters.
Results. — The proposed architecture embeds less convolutions, with much larger filters in the final convolutional layer, and is more general: it is able to deal with larger images and lower payloads. For the ''same embedding key'' scenario, our proposal outperforms all other steganalyzers, in particular the existing CNN-based ones, and defeats many state-of-the-art image steganography schemes. The information encoded by the final vector of features is so discriminating that the classifier part can be reduced to only two output neurons. We finally evaluated the detection ability of the CNN against two spatial domain steganographic schemes and a frequency domain one. More precisely, we designed a perfect steganalyzer for embedding payloads of 0.4 bit per pixel, and for all the steganographic tools investigated in this article (working either in spatial or in frequency domains). Rather interesting results have been obtained too, albeit to a lesser extent, for a payload value of 0.1 bpp.
Discussion and conclusions. — The obtained results are very encouraging, and they outperform all the previous deep learning proposals for steganalysis. A first step in the design of a universal detector has been achieved too, as we are able to detect HUGO based hidden messages even when a WOW steganographier has been used during the training stage. These results allow us to propose to add fragile watermarks on media like pictures or pdf medical documents, to guarantee the authenticity of the material: any attempt of modification of the support will alter the watermark, proving by doing so the modification. Another application is to add personal and medical information inside medical images.

MOTS CLÉS
Sécurité pour la télémédecine ;
Stéganographie ;
stéganalyse ;
Apprentissage approfondis

Résumé
Introduction. — La stéganographie, l'art de dissimuler de l'information au sein de médias numériques tels que les images et les vidéos, et la stéganalyse, sa contre-mesure tentant de détecter la présence d'une information secrète dans un document semblant innocent, sont fréquemment signalés comme étant des techniques de sécurité intéressantes pour la télémédecine. Au cours des dernières années, l'apprentissage profond (*deep learning*) a émergé dans la compétition entre stéganographie et stéganalyse, paraissant une alternative intéressante dans le cadre des stéganalyseurs basés sur des modèles raffinés d'image couplés avec des classifieurs d'ensembles. On peut alors combiner une sélection bien choisie de caractéristiques d'images avec des procédures innovantes de classification, au travers d'une approche d'apprentissage approfondie moderne appelée les réseaux de neurones convolutionnels (RNC). Ces réseaux, qui sont faits pour de la classification basée sur de la détection de variations dans les formes 2D, produisent la plupart du temps les meilleurs résultats dans divers problèmes de reconnaissance d'images.
Matériel et méthodes. — Nous avons programmé un stéganalyseur basé sur les RNC, pour des images stéganographiées avec une seule et même clé secrète. Le RNC proposé a une structure assez différente des réseaux développés jusqu'ici, et il est capable de fournir un fort taux de détection sur de nombreux logiciels de stéganographie, sous l'hypothèse que l'adversaire n'utilise qu'une seule clé d'embarquement. La partie « convolutionnelle » de notre approche commence par un filtrage global n'utilisant qu'un seul filtre, suivi par une seconde couche convolutionnelle, qui produit un ensemble réduit de caractéristiques de haute qualité (256 caractéristiques pour 512 × 512 pixels) grâce à l'utilisation de larges filtres.
Résultats. — L'architecture proposée embarque un plus faible nombre de convolutions que ce qui se trouve habituellement dans la littérature. Les filtres sont plus larges dans la dernière couche de convolution, et le réseau dans son ensemble est plus général : il permet de considérer des images plus larges, et de plus faibles taux d'embarquement. Pour le scénario d'une seule clé, nos résultats sont meilleurs que tous les autres stéganaliseurs, dont ceux basés sur des RNC, et nous pouvons mettre en échec de nombreux outils de stéganographie. L'information encodée par le vecteur final de caractéristiques est si discriminant, que la partie de classification peut se réduire à deux neurones de sortie. Nous avons finalement évalué la capacité de détection de notre RNC contre deux algorithmes de stéganographie fonctionnant dans le domaine spatial, et un dans le domaine fréquentiel. Nous avons obtenu un stéganalyseur parfait

Please cite this article in press as: Salomon M, et al. Steganalysis via a convolutional neural network using large convolution filters for embedding process with same stego key: A deep learning approach for telemedicine. Eur Res Telemed (2017), http://dx.doi.org/10.1016/j.eurtel.2017.06.001