Veri Gizleme için Derin Öğrenme Yöntemlerinin Kullanımı

Mehmet Zeki KONYAR

Yazılım Mühendisliği Bölümü / Mühendislik Fakültesi, Kocaeli Üniversitesi, Türkiye

mzeki.konyar@kocaeli.edu.tr

Özet **–** Veri gizlemede, resim, video, ses veya metin gibi bir taşıyıcı nesne içerisine belirli mesajlar gizlendikten sonra elde edilen yeni taşıyıcı alıcıya gönderilir. Steganografi ve damgalama şeklinde ikiye ayrılan veri gizlemede gizli haberleşme, içerik koruması ve kimlik doğrulaması gibi işlemler için çeşitli yöntemler bulunmaktadır. Gizli haberleşme amacıyla kullanılan veri gizleme yöntemlerinde gizli mesajı içeren taşıyıcı nesne orijinal nesneye çok benzer olup, üçüncü kişilerde herhangi bir şüphe uyandırmamaktadır. Klasik veri gizlemede resim ve videolar için geliştirilen ve veri gizleme kapasitesi, fark edilmezlik, saldırılara dayanıklılık gibi parametreleri iyileştiren birçok güncel yöntem bulunmaktadır. Bu yöntemlerde özellikle veri gizleme kapasitesinin sınırlara yaklaşması araştırmacıları farklı alanlara yönlendirmiştir. Derin öğrenme yaklaşımları kullanılarak yeni veri gizleme yöntemlerinin geliştirilmesi bunların başında yer almaktadır. Bu çalışmada öncelikle derin öğrenme modellerinin veri gizleme amacıyla kullanılma durumları ve derin öğrenmenin veri gizleme için kullanılmaya başlamasıyla ortaya çıkan yeni yaklaşımlar ve terimler değerlendirilmiştir. Daha sonra, evrişimsel sinir ağları (convolutional neural network; CNN) ve çekişmeli üretici ağlar (generative adversarial network; GAN) gibi farklı mimari yapılar ve bunların veri gizlemede kullanım durumları irdelenmiştir. Bu çalışma kapsamında son olarak, klasik veri gizleme kalite ölçütlerinin derin öğrenme temelli veri gizleme yöntemleri için kullanılmasının yanı sıra derin öğrenme mimarileri için kullanılan bazı kalite metriklerinin veri gizlemede kullanılabilme olanakları değerlendirilmiştir. Ayrıca derin öğrenme ile yapılan veri gizleme çalışmalarının, klasik yöntemlere göre avantajları, günümüzdeki bilgi güvenliği problemlerine nasıl çözümler getirdiği, gelecekte hangi problemlere uygulanabileceği üzerinde durulmuştur.

Anahtar Kelimeler – Bilgi Güvenliği, Derin Öğrenme, GAN, Steganografi, Veri Gizleme

Teşekkür: Bu çalışma Kocaeli Üniversitesi Yazılım Teknolojileri Araştırma Laboratuvarı (Star-Lab) imkanlarıyla gerçekleştirilmiştir.

The Use of The Deep Learning Methods for Data Hiding

Mehmet Zeki KONYAR

Software Engineering Department / Engineering Faculty, Kocaeli University, Türkiye

mzeki.konyar@kocaeli.edu.tr

Abstract **–** In data hiding, the new carrier is sent to the receiver after certain messages are hidden in a carrier object such as a image, video, sound or text. The data hiding, which is divided into two as steganography and watermarking, has various methods for processes such as secret communication, content protection and authentication. In data hiding methods used for secret communication, the carrier object which is contains

the secret message is very similar to the original object and does not arouse any suspicion to third parties. In classical data hiding, there are many up-to-date methods developed for images and videos that improve parameters such as data hiding capacity, invisibility, and resistance to attacks. fields One of them is the development of new data hiding methods using deep learning approaches. In this study, first of all, the use of deep learning models for data hiding and the new approaches and terms that emerged with the use of deep learning for data hiding were evaluated. Then, different architectural structures such as convolutional neural networks (CNN) and generative adversarial networks (GAN) and their usage in data hiding are discussed. Finally, within the scope of this study, the use of classical data hiding quality criteria for deep learning-based data hiding methods and the possibilities of using some quality metrics used for deep learning architectures in data hiding were evaluated. In addition, the advantages of data hiding studies with deep learning compared to classical methods, how they provide solutions to today's information security problems, and which problems they can be applied to in the future are emphasized.

Keywords – Information Security, Deep Learning, GAN, Steganography, Data Hiding

Acknowledgments: This study was carried out with the facilities of Kocaeli University Software Technologies Research Laboratory (Star-Lab).