6 Self-Correcting and Authentication Algorithm for Automotive Applications

6.1 Self-Learning Algorithms

For autonomous vehicle and future automotive applications, employment of self-learning algorithms for different purposes and use cases is of crucial importance. There are plenty of learning algorithms proposed in literature. Some of these are already finding their way into the automotive field and others are still in development. Some iterative self-learning algorithms for image processing were developed by the authors of the book themselves [1–3]. One of these iterative algorithms is described and discussed in this chapter. The algorithms are based on amalgamation of two fascinating fields, that is, coding and cryptography. More specifically, the forward error correction codes are combined with message authentication codes (MACs) to the benefit of both. The basic idea is to have cryptographic algorithms for data authentication which are tolerant to minor modifications, such as bit errors below a certain threshold. Such algorithms are very rare, however, some of these can already be found in literature. When these algorithms are combined with forward error correction codes and run in an iterative manner together with carefully tuning some parameters, then both fields benefit from the iterative process of error correction and authentication based on self-learning. As a result, the error correction capability of the employed forward error correction code gets better and in turn the data authentication results improve as well.

One of the aims of the self-learning algorithms described in this chapter is to enable improved error correction of the information protected using security mechanisms. Data or images exchanged between a vehicle and the backend (the OEM's systems and databases) is considered here as the information which needs to be processed and is protected by data authentication mechanisms. The data in general include text, audio and video; however, the algorithm described in this chapter is focused on images. Some important parts of the protected image, known as the landmarks, are considered as a region of interests (RoI) and are protected by their respective authentication tags. As a basis for learning property of the algorithm, an iterative corrective process based on turbo convolutional decoding is used in such a way that in every iteration, parts of the decoder's trellis path are learned by the algorithm. As a result, channel decoding results are improved with every iteration. Learning property of the algorithm is based on the knowledge gained from previous iterations of the algorithm, which is used in the current iteration for further improvement of decoding results. Additionally, iterative processes used for error corrections are supported by authentication tags, which are used as a measure of correction success.

Object recognition technology, including face recognition as a most frequently use case, is a biometric solution which measures and matches the unique characteristics

https://doi.org/10.1515/9783110629613-006