

الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي 08 ماي 5491. بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès



THESIS

To obtain the diploma of **Master**
Field: **Computer Science**
Specialty: **Intelligence Artificielle et Science des Données**

Theme

**Adversarial Embedding for Image Steganography:
A Theoretical Study of the Min–Max Protocol and the
Backpack Scheme**

Presented by:
Aymen Slimani

Submission Date: **September 2026**
In front of the jury composed of:

Dr. Taouli Amina
Dr. Amrane Abdelkader
Dr. Louhab Zouaoui

President
Supervisor
Examiner

Academic Year : 2025/2026

Abstract

Modern image steganography hides a secret payload by introducing changes that minimize a learned or hand-crafted distortion function, while a steganalyst tries to decide whether an image carries a message. When the steganalyst is a deep convolutional network, this becomes an adversarial game in which the embedder must remain undetectable against a set of detectors. The *min-max protocol* formalizes this game, but its instantiation with the ADV-EMB scheme is known to suffer from a structural flaw. The **Backpack** scheme of Bernard *et al.* (IEEE TIFS, 2022) repairs this flaw with a fully backpropagable adversarial embedding simulator that respects the payload constraint exactly.

This master’s report is the *theoretical* component of a two-part graduation project. It studies, in a self-contained way, the mathematical machinery behind adversarial embedding: the information-theoretic model of steganographic security, the distortion-minimization framework and its coding-theoretic limit, deep steganalysis detectors, adversarial examples, the min-max protocol and the flaw of ADV-EMB, and finally the Backpack construction itself, its differentiable embedding simulator, the entropy/payload constraint solved through a Lagrange multiplier, the implicit differentiation that makes the constraint backpropagable, and the Gumbel-based relaxation used to obtain gradients through discrete embedding changes. The companion engineering report presents the practical reproduction of the scheme.

Keywords, steganography, steganalysis, adversarial embedding, min-max protocol, Backpack scheme, distortion minimization, Gumbel-softmax, implicit differentiation, deep learning