Co-operative three Player Game Theory-based Machine Learning Techniques for an Adaptive Video Steganography Framework

1. Technology:

This technology introduces a cooperative game theory approach to enhance the video steganography framework. The framework involves three main steps: (1) Cover video creation, (2) Secret image pre-processing, and (3) Embedding. In the first step, the cover video is divided into segments using a scene change detection method. After segmentation, motion vectors are determined using the Block Matching Motion Estimation Algorithm (BMMEA), and the Region of Interest (ROI) is selected based on these vectors. The selected ROIs are then grouped according to their momentum. For additional security, the secret image is scrambled using the pixel-wise Arnold Transform in the next step. Finally, the scrambled secret data is embedded into the ROIs. An ideal video steganography system must ensure that the video quality remains intact after embedding the secret data. Key quality factors include perceptual invisibility, payload capacity, and robustness, though these factors often conflict. To resolve this issue, a machine learning-based optimization approach is used. A cooperative 3-player game theory model is proposed, where each quality factor acts as a player. The optimal solution for the framework is found using the Iterative Elimination of Strictly Dominant Strategies (IESDS) method, resulting in the best trade-off between these conflicting quality factors. Figure 1 represents a complete framework of the proposed technology.

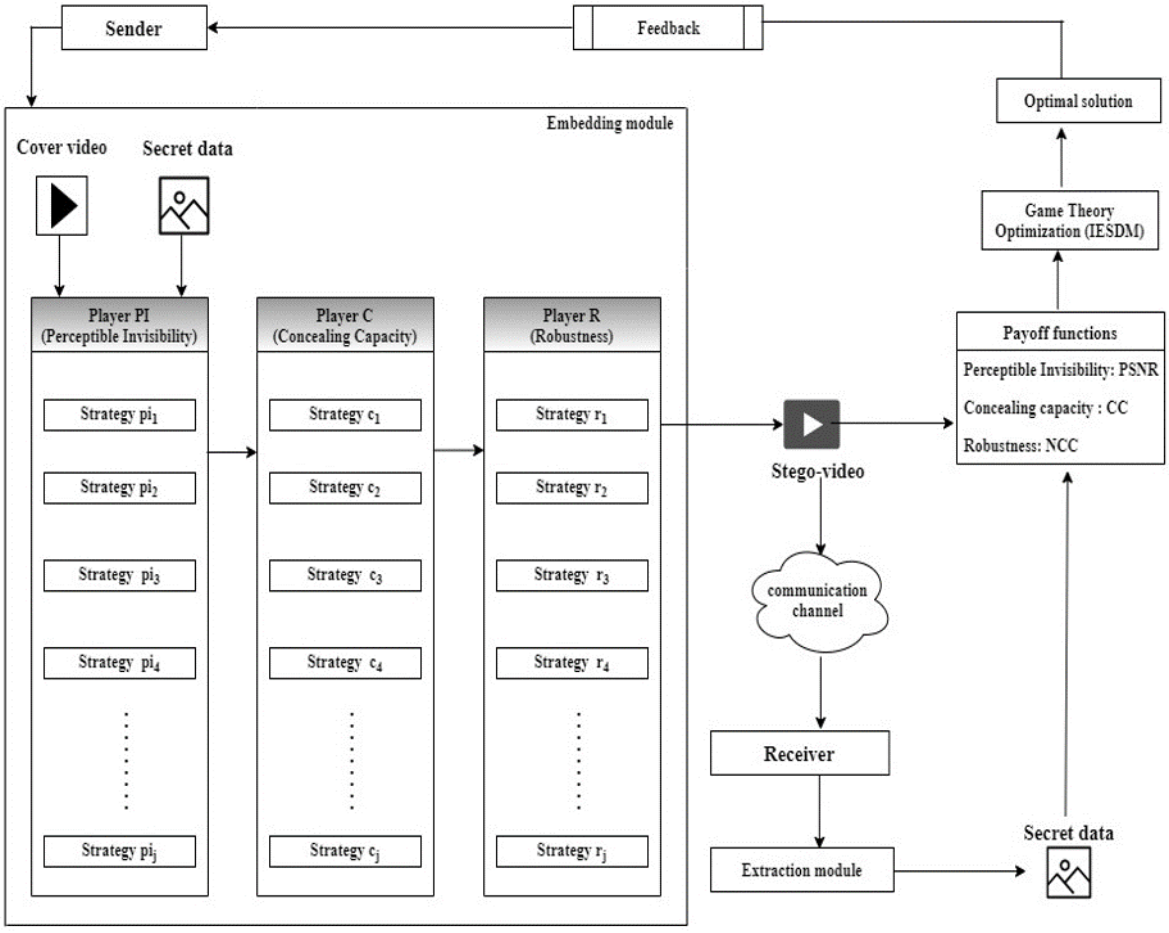

Figure 1. The comprehensive framework of the proposed game theory-based video steganography approach

2. Problem Addressed:

Previous research on game theory-based steganography has primarily focused on two strategic players. In contrast, the proposed video steganography approach introduces a three-player game. This approach addresses the challenge of improving and balancing key quality factors—such as perceptual invisibility, concealment capacity, and robustness of the stego-video. A game model is developed to find an optimal solution for this issue. Using game theory principles, an optimal solution is derived through a game matrix, with the game being structured as a dynamic cooperative model. The proposed game allows for the analysis of various scenarios to reach an optimal outcome. Notably, this game theory-based video steganography model offers the following unique features:

- It involves three players.
- It is a mixed-strategy cooperative game.
- It enhances and maintains a trade-off between the quality factors by applying game theory to achieve the best solution for all players.

3. Industrial Applications:

In the field of internet communication, secure data transmission is a primary goal across various sectors, often achieved by hiding data within common media. Steganography plays a crucial role in areas such as the military, healthcare, corporate environments, and multimedia, where covert communication is essential for both internal and external security purposes.

4. Patent Application Number: 202441021933