Ali et al., (2023)[1] demonstrated a unique method for video steganography, involving the use of a genetic algorithm (GA) to identify the Region Of Interest (ROI) in the cover video. The Region Of Interest (ROI) was identified as the most suitable area in the movie for data embedding. The secret material was encrypted using the widely recognized Advanced Encryption Standard (AES) and inserted into the cover video, utilizing no more than 10% of the footage. This method ensured the confidentiality and security of the embedded data. The recommended technique was evaluated using Peak Signal-to-Noise Ratio (PSNR) and encoding and decoding time as performance metrics. The findings showed that the recommended technique had a high level of efficiency and capacity for embedding data, as shown by a PSNR range of 64 to 75 dBs. This means that it is extremely difficult to distinguish the embedded data from the original video.

Suresh et al.,(2022)[2] explored the optimised approach which was determined the optimal region by considering factors such as energy, coverage, intensity, and kurtosis. Encrypting the secret information in advance enhanced the recommended method. Lastly, the Lifting Wavelet Transform (LWT) was employed to conceal concealed data within the wavelet coefficient framework on pivotal frames. The evaluation of performance was conducted using three metrics: Peak Signal-to-Noise Ratio (PSNR), Embedding Capacity, and Normalised Correlation (NC). The recommended approach achieved enhanced security and imperceptibility for high video quality, with a sound level of 75.141 dB and an embedding capacity of 70.8%.

Sharath et al.,(2022)[3] created a secure video steganography data transfer system. After converting the test video into frames, each frame was processed. Then, the GSO (Glow-worm Swarm Optimization) algorithm selected the best frame pixels. The confidential data was encrypted using the OHE (One-Hot Encoding) model and the keys were optimally created using JOA(Jaya Optimization Algorithm), boosting secrecy. A rigorous experimental validation on the benchmark test video showed that the OMPS (Optimized Multi-Pixel Selection),HEVS (Hybrid Encryption Video Steganography) methodology outperformed other methods. Video 1 ECs were 85.05 percent for OMPS-HEVS, 58.60 percent for simple LSB, 62.27 percent for OMSB, 65.80 percent for Knight Tour, and 71.20 percent for FGWO-MOC. OMPS-HEVS increased EC by 79.10% in the video.

Almomani et al.,(2022)[4] suggested steganography approach involves partitioning the private ransomware data and the cover High-Efficiency Video Coding (HEVC) frames into separate blocks. The gathered data provide evidence of the efficacy of the proposed steganography technique, as it achieves a significant storage capacity and successfully embeds the buried malware among video frames without detection. The findings demonstrated that the proposed model achieved a maximum signal-to-noise ratio of 59.3 dB and a mean-square-error of 0.07 for the examined HEVC streams. In addition, none of the 65 antivirus engines were capable of detecting the existence of the integrated ransomware program.

Dhawan et al., (2021) [5] proposed a method of image steganography, utilized a range of strategies to augment the security of the confidential information. This was accomplished by employing a Binary Bit-Plane Decomposition (BBPD) picture encryption approach. The Salp Swarm Optimization Algorithm (SSOA) was subsequently proposed as a revolutionary way to improve the payload capacity by employing an adaptive embedding process. The SSOA algorithm was utilized to precisely ascertain the location of the border and efficiently mitigate the abnormalities in the blocks. The proposed steganography approach exhibited superior results in terms of security, image quality, and payload capacity compared to the present state-of-the-art technology.

Abbas et al.,(2015)[6] regarding video steganography, Yang and Deb developed the 2009 meta-heuristic search algorithm (CS) Cuckoo Search. It was based on cuckoo mating behaviours. The suggested approach relied on bit-by-bit sensitive data extraction. Rearranging byte bits yielded five forms. Next, find the best cover frame carrier pixel. The Euclidean distance determined the best pixel by comparing it to several byte formats. Pixels were randomly moved using Lévy flight random walk. The 3-3-2 Least Significant Bit (LSB) replacement algorithm then found and merged the carrier pixel into its RGB components. In terms of Peak Signal to Noise Ratio (PSNR), the results demonstrated that Cuckoo Search outperformed both the Genetic Algorithm (GA) and the basic approach.

Dasgupta et al.,(2013) [7] developed video steganography approach which was employed using a 3-3-2 LSB based scheme as the foundation. The evaluation of any steganographic technique was intended to be based on two crucial factors: imperceptibility and video quality. Therefore, the fundamental method was improved by using a Genetic Algorithm (GA) that aimed to get the highest level of imperceptibility for concealed data. An anti-steganalysis test was employed to ascertain the innocence of the frame in relation to the original frame. The experimental findings demonstrated a significant enhancement in both the Peak Signal-to-Noise Ratio (PSNR) and Image Fidelity (IF) values following the optimization of the basic approach.

References

Ali, Nizheen A., and Ramadhan Mstafa. "Optimizing Region of Interest Selection for Effective Embedding in Video Steganography Based on Genetic Algorithms." *Computer Systems Science and Engineering* 47, no. 2 (2023).

Suresh, Meenu, and I. Shatheesh Sam. "Optimized interesting region identification for video steganography using Fractional Grey Wolf Optimization along with multi-objective cost function." *Journal of King Saud University-Computer and Information Sciences* 34, no. 6 (2022): 3489-3496.

Sharath, M. N., T. M. Rajesh, and Mallanagouda Patil. "Design of optimal metaheuristics based pixel selection with homomorphic encryption technique for video steganography." *International Journal of Information Technology* 14, no. 5 (2022): 2265-2274.

Almomani, Iman, Aala AlKhayer, and Walid El-Shafai. "Novel Ransomware Hiding Model Using HEVC Steganography Approach." *Computers, Materials & Continua* 70, no. 1 (2022).

Dhawan, Sachin, Chinmay Chakraborty, Jaroslav Frnda, Rashmi Gupta, Arun Kumar Rana, and Subhendu Kumar Pani. "SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT." *IEEE Access* 9 (2021): 87563-87578.

Abbas, Sameh A., Taha IB El Arif, Fayed FM Ghaleb, and Sohier M. Khamis. "Optimized video steganography using Cuckoo Search algorithm." In *2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, pp. 572-577. IEEE, 2015.

Dasgupta, Kousik, Jyotsna Kumar Mondal, and Paramartha Dutta. "Optimized video steganography using genetic algorithm (GA)." *Procedia Technology* 10 (2013): 131-137.