



High-Capacity Coverless Steganography Using Pixel Gradient Analysis

Aditya Ghosh¹ , Md Sayeef¹, Aritra Kumar Patra¹ , Pabak Indu^{2,3,4} ,
and Souvik Bhattacharyya¹

¹ Department of CSE, University Institute of Technology, The University of Burdwan,
Bardhaman, West Bengal 713104, India

² Department of CSE (AIML) & CSBS, Institute of Engineering and Management, University
of Engineering and Management, Kolkata, West Bengal 700091, India
pabakindu@yahoo.co.in

³ IEM Centre of Excellence for Cloud Computing and IoT, Department of CSE (AIML) &
CSBS, , Institute of Engineering and Management, Kolkata 700091, India

⁴ IEM Centre of Excellence for Data Science, Department of CSE (AIML) & CSBS, Institute of
Engineering and Management, Kolkata 700091, India

Abstract. Since the dawn of Internet, we have been able to do so much more work in a fixed amount of time. As time passed, the technologies involved became faster and more efficient in transmission and processing of data. Nowadays important information's like banking details and passwords are saved digitally within a computer. As more and more people are using internet for communication and other requirements, they are becoming vulnerable to cyber-attacks. Safety and security of personal data has become utmost priority at this point. Tools like steganography become useful in this regard.

We will be looking at a coverless image steganography method leveraging pixel gradient analysis to securely embed data into synthetic images. The process utilizes StyleGAN2 with Adaptive Data Augmentation (ADA) to generate synthetic images. This method focuses on RGB images, splitting them into their respective R, G and B channels and further subdividing the images layers into smaller cells. Every cell is used to map a particular portion of the secret information. Since this technique uses mostly mapping and only requires modification, when necessary, the amount of data that gets changed or manipulated is very less. The technique ensures minimal changes to the image, keeping modifications below 2 values every 9 values in the worst case. The proposed method can be highly scalable and secure solution for hiding large amounts of data without drawing attention, as it doesn't modify the image's visibly distinct features. It proves robust against steganalysis tools and offers higher capacity and security compared to prior models, making it an ideal approach for covert data transmission.

Keywords: StyleGAN2 · Steganography · Coverless