Review of image watermarking methods for modern world applications

Mikołaj Kordowski Adam Pilewski

Warsaw University of Technology, Faculty of Electrical Engineering

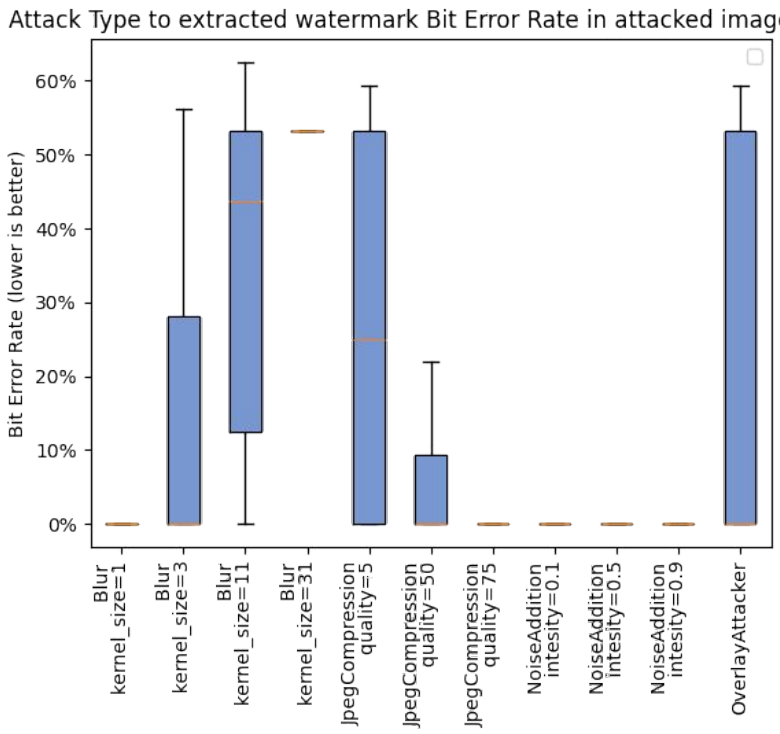
INTRODUCTION

In the era of AI and social media, digital media security and authenticity have become increasingly important. Over **3.2 Billion images** are shared daily. Watermarking techniques are a crucial tool in protecting content from unauthorized modifications and to ensure traceability. This study compared different watermarking algorithms, including **RivaGAN (a deep learning-based approach)** and classical methods like **DWT-DCT, DWT-DCT-SVD, and a Naïve approach**. The evaluation focused on their robustness against attacks and practical usage.

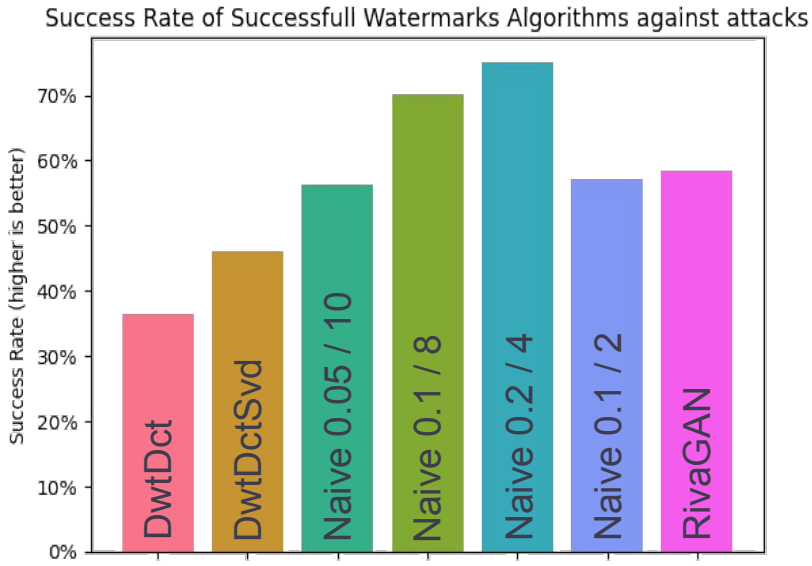
METHODOLOGY

To collect data each image in our dataset had a watermark added (encoding) and then attacked using various algorithms such as **Blur, Noise, lossy compression**. After each step the watermark was extracted (decoding) to compare how robust the encoding and attacking algorithms were respectively. For more in depth statistics different metrics were used such as SSIM or **Bit Error Rate (BER)**.

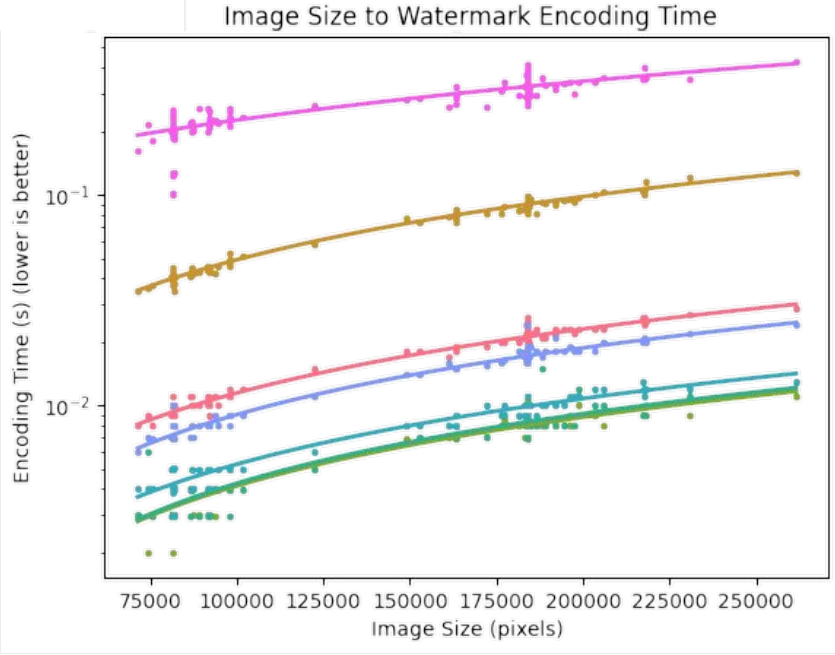
RESULTS



The box plot visualizes the Bit Error Rate (BER) of extracted watermarks after various attacks, where higher values indicate greater degradation. A value of 50% means total watermark data loss. JPEG compression, overlay attack, and strong blur significantly impacted watermark extraction, while noise-based attacks had little effect.



The success rate visible on the chart above shows that higher values indicate better resilience. **RivaGAN performs acceptably,** which is consistent with its original research. The naïve approach had the highest success rate likely because it used the source image for decoding, making extraction more reliable.



RivaGAN performed the worst in terms of encoding time, whereas the naïve algorithm was the fastest.

CONCLUSIONS

- Algorithms using source image during decoding may cause image quality loss (lowest SSIM) but offer **great encoding speed and robustness**
- RivaGAN does not scale like the other algorithms, with decoding time increasing faster than encoding as image size grows
- JPEG compression and blur had a major impact on watermark persistence
- Adding noise did not affect watermarking

Warsaw University of Technology