Multimedia Tools and Applications (2023) 82:20497–20516
https://doi.org/10.1007/s11042-022-14301-0

A novel steganographic technique for medical image using SVM and IWT

Partha Chowdhuri[1] · **Pabitra Pal**[2] · **Tapas Si**[3]

Received: 25 May 2022 / Revised: 11 November 2022 / Accepted: 10 December 2022 /
Published online: 6 January 2023

Abstract

This study presents an efficient authentication scheme for digital image steganography on medical images benefiting from the combination of both techniques: Support Vector Machine (SVM) and Integer Wavelet Transform (IWT). We use two different strategies in this paper, where SVM is used first to separate the Region of Interest (ROI) from Non-Region of Interest (NROI) in the medical image. Then IWT is applied to embed secret information within the NROI part of the medical image (Cover Image). Moreover, we have applied a circular array and a shared secret key to enhance the robustness of the proposed scheme. The research looked into the various experimental analyses to establish the acceptability of the existing scheme. The simulation is performed to measure the imperceptibility using Peak Signal to Noise Ratio (PSNR) and to test the robustness using the Structural Similarity Index Measure (SSIM). The experimental result shows good imperceptibility with a PSNR of 64 dB and better robustness with a SSIM of 0.96 for the proposed steganographic scheme.

Keywords Steganography · Integer wavelet transform · Support vector machine · Circular array · ROI & NROI · Medical image

Partha Chowdhuri and Tapas Si contributed equally to this work.

✉ Pabitra Pal
pabipaltra@gmail.com

Partha Chowdhuri
prc.email@gmail.com

Tapas Si
shritapassi.ai@gmail.com

[1] Computer Science, Vidyasagar University, Vidyasagar University Road, Paschim Medinipur, 721102, West Bengal, India

[2] Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Simhat, Haringhata, 741249, West Bengal, India

[3] Department of Computer Science and Engineering, Bankura Unnayani Institute of Engineering, Pohabagan, Bankura, 722146, West Bengal, India

1 Introduction

The pandemic of COVID-19 has emphasised the significance of the Internet and multimedia technology. We are becoming more agnostic to internet communication technologies as we share private information such as health information, bank details, credit card data, or family pictures via the internet in our daily lives. Nowadays, sharing this personal or commercial information over the internet is a high risk activity. Unauthorized use, tampering, and copy-right violations may happen very easily as the information is transmitted over an untrusted digital platform. Authentication and confidentiality are very much needed to defend against unauthorised access and usage. So users need a trustworthy platform or application through which they can easily share their personal information without any doubt. In this scenario, a joint venture of steganography and machine learning may provide an efficient and effective solution. In the existing steganographic model, the embedding position remain same in each and every image used as cover. It does not depend on a type of the image we are using. But in the proposed model, the embedding position depends on the type of the image. With the help of machine learning, it finds the non region of interest (NROI) and embeds the secret information there. It not only makes the embedding process dynamic but also ensures that the region of interest of every image remain unchanged even after embedding secret bits in the image. In this study, we proposed a robust steganographic scheme using Support Vector Machine (SVM) and Integer Wavelet Transform (IWT) to improve security and robustness while maintaining authenticity and data integrity.

Medical images are more typical than any other ordinary images since they store a patient's valuable information for diagnosis purposes. Such images need more security and confidentiality as total diagnosis depends on it. In tele-medicine applications, the transmission of medical images via an open channel demands strong security and copy-right protection. So we always have to take care of these images while embedding the secret information into them. To do so, a medical image is classified into two regions; an important part of the medical image used for diagnosis purposes is known as the Region of Interest (ROI), and the rest of the image, which is not so essential, is known as the Non Region of Interest (NROI). A small mis-classification may cause big trouble in extracting essential information of the patient. In statistical learning theory, SVM is a new class of machine learning method that can be used as an image classifier. Applying SVM in the transform domain for medical image watermarking is still an open area of research.

Steganography in medical images can be performed in three stages. The first stage can be described as the classification of NROI and ROI; the second stage is stego embedding in the host image in the transform domain; and the last stage is the extraction of embedded information. The machine learning algorithm named SVM is being used, which is widely used for classification problems. On the other hand, the transform domain methods such as Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Integer Wavelet Transform (IWT) are robust against various attacks in the embedding and extraction processes. However, among all these schemes, the IWT has the special property that it can transform the pixel values into some integer values, which might be very useful for designing a reversible steganographic model.

In the proposed model, a double layer of security is introduced to ensure the robustness of embedded data. The embedded data is scrambled using a unique key. The transform domain based hybrid steganographic technique is applied to embed the scrambled data into the IWT coefficients of the host image. The proposed scheme exploits the reversibility feature of IWT and the randomization property of the circular array.