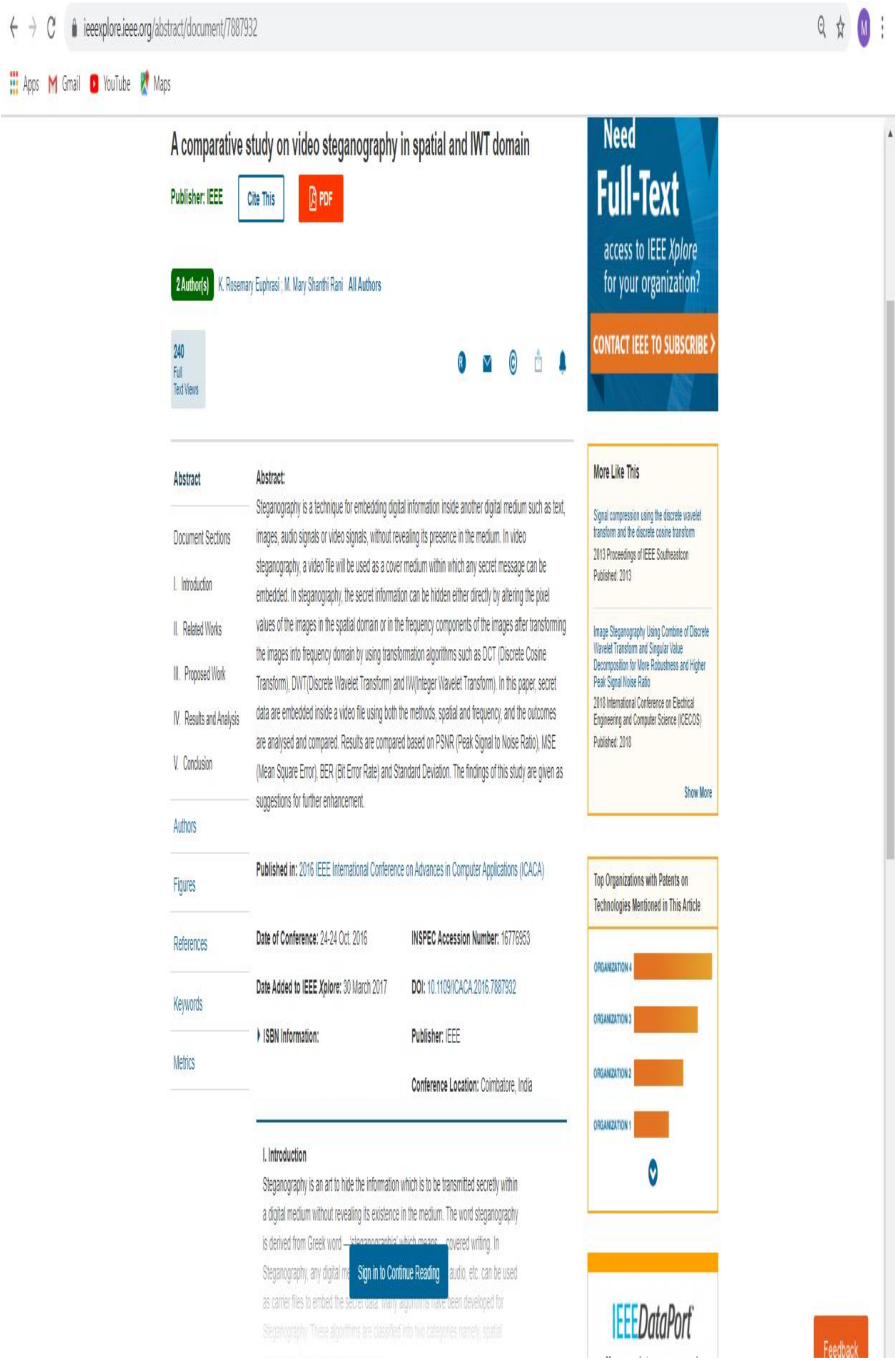

A comparative study on video steganography in spatial and IWT domain

Publisher: IEEE

2 Author(s) K. Rosemary Euphrasi ; M. Mary Shanthi Rani All Authors

Abstract:
Steganography is a technique for embedding digital information inside another digital medium such as text, images, audio signals or video signals, without revealing its presence in the medium. In video steganography, a video file will be used as a cover medium within which any secret message can be embedded. In steganography, the secret information can be hidden either directly by altering the pixel values of the images in the spatial domain or in the frequency components of the images after transforming the images into frequency domain by using transformation algorithms such as DCT (Discrete Cosine Transform), DWT(Discrete Wavelet Transform) and IW(Integer Wavelet Transform). In this paper, secret data are embedded inside a video file using both the methods, spatial and frequency, and the outcomes are analysed and compared. Results are compared based on PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), BER (Bit Error Rate) and Standard Deviation. The findings of this study are given as suggestions for further enhancement.

Published in: 2016 IEEE International Conference on Advances in Computer Applications (ICACA)

Date of Conference: 24-24 Oct. 2016

INSPEC Accession Number: 16776953

Date Added to IEEE *Xplore*: 30 March 2017

DOI: 10.1109/ICACA.2016.7887932

ISBN Information:

Publisher: IEEE

Conference Location: Coimbatore, India

More Like This

Signal compression using the discrete wavelet transform and the discrete cosine transform
2013 Proceedings of IEEE Southeastcon
Published: 2013

Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio
2018 International Conference on Electrical Engineering and Computer Science (ICECOS)
Published: 2018

Show More

Top Organizations with Patents on Technologies Mentioned in This Article

I. Introduction

Steganography is an art to hide the information which is to be transmitted secretly within a digital medium without revealing its existence in the medium. The word steganography is derived from Greek word —'steganographic' which means covered writing. In Steganography, any digital me audio, etc. can be used as carrier files to embed the secret data. Many algorithms have been developed for Steganography. These algorithms are classified into two categories namely, spatial

2016 IEEE International Conference on Advances in Computer Applications (ICACA)

A Comparative Study On Video Steganography in Spatial and IWT Domain

K.Rosemary Euphrasi
Dept. of Computer Science
Fatima College
Madurai, India
rmeuph@yahoo.com

M. Mary Shanthi Rani
Dept. of Computer science and Applications,
Gandhigram Rural Institute, Deemed University
Gandhigram , Dindigul, India
drmaryshanthi@gmail.com

Abstract—**Steganography is a technique for embedding digital information inside another digital medium such as text, images, audio signals or video signals, without revealing its presence in the medium. In video steganography, a video file will be used as a cover medium within which any secret message can be embedded. In steganography, the secret information can be hidden either directly by altering the pixel values of the images in the spatial domain or in the frequency components of the images after transforming the images into frequency domain by using transformation algorithms such as DCT (Discrete Cosine Transform), DWT(Discrete Wavelet Transform) and IW(Integer Wavelet Transform).. In this paper, secret data are embedded inside a video file using both the methods, spatial and frequency, and the outcomes are analysed and compared. Results are compared based on PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), BER (Bit Error Rate) and Standard Deviation. The findings of this study are given as suggestions for further enhancement.**

Keywords—IWT; LSB Substitution; RGB Domain; Steganography; Video Steganography

I. INTRODUCTION

Steganography is an art to hide the information which is to be transmitted secretly within a digital medium without revealing its existence in the medium. The word steganography is derived from Greek word —'steganographia' which means —covered writing. In Steganography, any digital medium such as images, text, video, audio, etc. can be used as carrier files to embed the secret data. Many algorithms have been developed for Steganography. These algorithms are classified into two categories namely, spatial domain and Frequency domain techniques.

Spatial domain techniques are very simple and easy to implement. More amount of information can be hidden without much difficulty [1]. LSB (Least Significant Bit) substitution is the most commonly used method for hiding data in the spatial domain. In this method, few least significant bits of the pixels of the cover image are replaced by the bits of secret data. Replacing few least significant bits of the pixels does not create significant visual change in the image. Since the change is very less it is invisible to the human visual system. At the same time if a hacker suspects the presence of the message, then he can trace the message without much difficulty by gathering all the least significant bits of the pixels from the image [2]. Various algorithms such as Selected LSB (SLSB), Dynamic hiding, Pixel Value Differencing (PVD) and Pixel Indicator Technique (PIT) have been developed to overcome this problem.

In Transform domain technique, instead of hiding the secret message directly in the pixels, messages are embedded in the frequency coefficients of the image. For this, some mathematical transformations such as Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) are applied to the image to transform it into frequency components. After transformation, the secret message is hidden in the frequency coefficients. Security can be boosted by hiding the data in selected frequency coefficients based on some threshold value. Then the image will be transformed back into spatial domain by inverse transformation.

The objective of this paper is to develop two algorithms for video steganography, one in spatial domain another in the frequency domain, and to compare their performances based on some standard criteria. In the spatial domain algorithm, a true colour image is separated into Red, Green, and Blue channels and data are hidden in any two channels at random using LSB substitution method. In the transform domain algorithm, a true color image is transformed into IWT (Integer Wavelet Transform) domain using a wavelet called 'haar' wavelet. The wavelet transforms the image into four frequency bands, namely AC, HC, VC, and DC. The band AC is the approximation coefficient band and the other three are detail coefficients. The secret data are embedded in the DC component and the image is transformed back into original form by reverse transformation.

Video Steganography is the art of embedding message inside the frames of a video in such a way that it does not make any visible distortion. Using a video file as a cover medium increases the volume of storage as well as it increases the complexity of sensing the presence of a secret message.

This paper is organised as follows. In Section 2 the papers which are referred for this work are reviewed. Section 3 presents the method of the proposed algorithm in detail and the experimental results and their evaluation are presented in section 4. Finally, conclusions appear in Section 5.

978-1-5090-3770-4/16/$31.00©2016 IEEE