Performance of Secured and Robust Watermarking Using Evolutionary Computing Technique

B.V.D. S. Sekhar, Research Scholar, Department of CS&SE, Andhra University, Visakhapatnam, India
P.V.G.D. Prasad Reddy, Department of CS&SE, College of Engineering, Andhra University, Visakhapatnam, India
G.P.S. Varma, SRKR Engineering College, Chinnamiram, India

ABSTRACT

Watermarking emerged as versatile technique of hiding confidential or copy right protect information. The image embedded with watermark is often prone to several security vulnerabilities due to several attacks. It is desired to secure the information in the form of watermark by making it immune to these attacks. Several techniques are prevailing which use image transform techniques for efficient watermark de-noising and extraction. However, in the recent past the evolutionary computing techniques evolved as promising methods. In this paper, one such attempt of integrating the popular image transform techniques with PSO for developing efficient watermarking scheme. Embedding and extraction of the watermark are demonstrated and finally the efficiency of the technique is evaluated in terms of calculated PNSR. Gray scale image is used as WM image and a color image is considered for hosting the WM image. The technique utilises only one frame of the color image for hiding securely the WM image instead of conventional method of using all the three frames.

KEYWORDS

De-Noising, DWT, Evolutionary Computing, PSO, Secured Watermarking

1. INTRODUCTION

With the revolution of modern wireless communication there is a drastic breakthrough in the personal communication systems. This led to huge exchange of digital data between multimedia devices. Digital cameras, camcorders and scanners are some such devices to list. With these digital devices it is clear that it is possible to generate multimedia data in the form of pictures and videos (Bender et al., 1996; Fotopoulos et al., 2003; Potdar et al., 2005; Liu et al., 2005). As a result, for a reliable transmission and security of this digital data, several efficient compression algorithm and techniques for high speed and secured transmission are proposed. The concern of digital data is due to several advantages like good quality, ease of editing, simple storage technique and very simple mode of exchange without much loss in the data with better fidelity. However, in spite of these advantages, the digital multimedia data several suffer with ownership and originality certifications. The advantages, the digital multimedia data severely suffer with ownership and originality certification. The advantages discussed above are even favourable for easy duplication and further manipulation. This is often considered as a severe threat to the genuineness of the data and easily prone to misuse of the same. Considering this, it is suggested to verify the originality and reliability of the digital data while processing transmission and exchange of it.

DOI: 10.4018/JGIM.2017100105

Copyright © 2017, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
It is the need of trending digital world that the owner of the digital data could ensure its ownership of it. Secured and protected against several unintended and illegal infringements. This scenario leads to deliberations concluding the need of a technology which can promise copy rights and avoid piracy of the digital data. The technology also should be capable of restricting the attempts of media pirates. In the recent past, several solutions were proposed to protect and secure multimedia data from piracy and unauthorised usage. This has been a challenging task for the researchers as it involves in several various solutions, one vital technique emerges as successful method of ensuring data protection. This technique involves in embedding secret data that significantly promotes the ownership of the multimedia in invisible form with the original digital media. This technique of hiding copy right certificate in the original data comes with different names like cryptography, steganography and water marking (Oliveira et al., 2002; Adesina et al., 2010). These are considered as subclasses of data security. Each method adopts unique technique for hiding the invisible data. Cryptography (Schneier, 1996; Koch et al., 1995; Anderson et al., 1996) technique involves in encryption and decryption. The multimedia or the digital data is encrypted with a key known as decryption key. Only the original owner or the consumer in genuine will be holding the decryption key. However, this technique failed to control the infringements often the decryption takes place as the data is open to the world. Steganography on the other hand uses cryptographic algorithms to secure the digital data. This method is proved to be volatile and hot adaptive. The third popular method known as water marking (WM). This technique is considered to be robust when compared with the other two methods stated above. This WM technique ensure protection of digital data and its security against several 1D, 2D and 3D signal processing attacks. Hence WM, emerged a reliable mode of data transfer by which the multimedia data like image and video can be transferred and further distributed preserving the ownership over internet and public media. Considering the above, the current work focuses on WM based techniques for protecting color images.

The objective of the proposed work includes developing intelligent digital WM method that protects the color images from various known attacks. The proposed technique uses the advantages of DWT for watermarking while the PSO is employed to enhance the performance of the same which is analysed in the presence of several watermark attacks. The proposed technique of digital WM ensures high degree of security interns of copyright protection, data authentication, finger print security, monitoring widely broadcasted data, confidential communication etc.

Further, certain emphasis is also been given to WM based copyright protection (Mintzer et al., 1998; Cox et al., 2000; Cox et al., 2001; Darwish et al., 2011; Bianchi et al., 2013) which is considered as the main motivation to this proposed work. In copyright protection process, certain invisible data is embedded into the original host object without much loss in the quality of the original data object. The embedded WM object may not prevent the data disclosure but protects the data ownership by providing embedded certificate which can be further used to claim the ownership of the original digital data. The proposed design cites several problems as well as demands associated with WM method. However, the main objective is to enhance PSNR. Other parameters like transparency, robustness and capacity can be further ensured with the basic interference provided by the proposed work. In this paper, evolutionary computing technique known as PSO is applied along with transform principles in watermarking. The choice of PSO has several advantages over other existing evolutionary tools in terms of quick convergence. Moreover, in PSO all the particles provide similar solution during convergence which states that the solution obtained is the best possible.

Further, the paper is organised as follows. Brief introduction to the watermarking methods and other known attacks is discussed in Section 2. Description of methods and techniques employed for watermarking is given in Section 3. The methodology proposed for watermarking is given in Section 4. Results of the simulation based experimentation are provided in Section 5. Overall conclusions are mentioned in Section 6.
Relationship of Some Organizational Factors to Information Systems Effectiveness: A Contingency Analysis of Egyptian Data
www.igi-global.com/chapter/relationship-some-organizational-factors-information/4540?camid=4v1a

A Case Study of IT Chargeback in government Agency
www.igi-global.com/chapter/case-study-chargeback-government-agency/6299?camid=4v1a