International Journal of Soft Computing 11 (2): 100-102, 2016
ISSN: 1816-9503

Protecting Digital Images for Identification and Authentication by Enhanced Discrete Wavelet Transform Watermarking Method

[1]Abdul Samad Shibghatullah and [2]Ali Jumaah Ali Alkaabi
[1]Faculty of Information and Communication Technology, University Teknikal Malaysia,
Hang Tuah Jaya Tungal, 76100 Durian, Melaka, Malaysia
[2]Ministry High Educatin of Iraq, Baghdad, Iraq

Abstract: The rapid growth of the internet increases access to multimedia data tremendously. Due to its growth and availability of multimedia computing facilities, the enforcement of multimedia copy write protection becomes an important issue. Digital content can be reproduced, without loss of quality but they may also be easily modified and sometimes imperceptibly. In many contexts, any alteration of image, audio, video data must be detected. Therefore, there need some works to develop security systems to protect the content of digital data. Digital watermarking is viewed as an effective way to detect content users from illegal distributing. There are research challenges about this area of research that still needs to be solving such as imperceptibility, robustness, security in the images. The objective of this study are 3-fold to investigate the strength and limitations of current watermarking schemes, to design and develop new schemes to overcome the limitations and to evaluate the new schemes using application scenarios of copyright protection, tamper detection and authentication. We focus on geometrically robust watermarking and semi-fragile watermarking for digital images. The proposed hybrid schemes that combine the strength of both robust and semi-fragile watermarks are studied. The proposed method which operates in hybrid wavelet domain, embeds information in the LH blocks of the wavelet transform of the image. After embedding, the watermark is adapted to the image by exploiting the masking characteristic of human visual system thus, showing the invisibility of watermark. By knowing the properties of embedding sequence, the mark can be reliably extracted without resorting to the original uncorrupted image.

Key words: Watermarking, wavelets, embedding, extraction, security, strength

INTRODUCTION

"There is a single light of science and to brighten it anywhere is to brighten it everywhere" Isaac Asimov (1920-1992). The rapid growth of the internet increases access to multimedia data tremendously. Due to its growth and availability of multimedia computing facilities, the enforcement of multimedia copy write protection becomes an important issue. Digital content can be reproduced, without loss of quality but they may also be easily modified and sometimes imperceptibly. In many contexts, any alteration of image, audio, video data must be detected. Therefore, there need some works to develop security systems to protect the content of digital data. New algorithms are proposed and analyzed to see the system's performance effectiveness and potential for future improvement (Ahmidi and Safabakhsh, 2004).

We know that one of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently and with a very high quality and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Digital media offer several distinct advantages over analog media. The quality of digital audio, images and video signals are higher than that of their analog counterparts. Editing is easy because one can access the exact discrete locations that need to be changed.

Motivation: The digital representation of text, audio, image and video documents has become very popular in the last decade. The success of digital technology is largely due to the capabilities of efficient transmission, storage and perfect copying (Arnold *et al*., 2003; Barni *et al*., 1999). However, especially the last feature leads to severe problems because unauthorized copying is also simplified. One approach to combat this problem is to mark a digital document such that a copyright can be proven or the

Corresponding Author: Abdul Samad Shibghatullah, Faculty of Information and Communication Technology, Uniuversity of Hang Tuah Jaya, 76100 Durian, Tungal, Melaka, Malaysia

distribution path is traced. Digital watermarking is expected to be a perfect tool for protecting the intellectual property rights. "Digital Watermarking" means embedding information into multimedia data that should be imperceptible but irremovable. Thus, in contrast to copyright information included in the header of the data streams, embedded watermarks remain in the document even after format conversions or D/A and A/D conversions. Two important applications of digital watermarks are resolving ownership disputes and distinguishing between different copies. In the first application the embedded watermark should uniquely indicate the originator of the document. In the second application, different watermarks are embedded into different copies of the same document. These marks are also called "digital fingerprints". Therefore novel watermarking techniques are used to solve certain problems in image authentication, The new approaches is able to detect as well as localize, malicious alterations, while offering robustness to image compression.

Problem statement: Digital watermarking algorithms are effectively applied to associated broadcast monitoring systems and copy control applications. In combination with digital rights management systems, these techniques can solve the bottleneck of the intellectual property dilemma in audio and image-related business areas. In an early stage of watermarking, users considered resisting to geometric attacks as an advantage of one technique over alternative implementations. For feature-based watermarking schemes, however, surviving geometric attacks is a precondition. The past 10 year have witnessed a important advancement in people recognizing of geometrical attacks and methods for surviving them. Some approach proposed particular types of attacks, although just a few of watermarking methods in fact, survived the huge set of potential variations of combined approaches. Even afterwards, many researchers identifying of these threats which the attacks compel on the performance of existent and upcoming methods are limited. It may just reflect the limitations of efficient benchmarking procedures and theoretical grounds for evaluating them. Cox *et al*. (2001) proposed a spread spectrum watermarking scheme based on Discrete Cosine Transform (DCT). The scheme aims to hide Gaussian distributed noise-style watermarks. But these noisy style watermarks may not offer any resistance for compressing the image data or for low-pass filtering attacks. Lee *et al*. (2008) presented a Genetic Algorithm-Based watermarking algorithm in the discrete wavelet t ransform domain. Wavelet-domain low-frequency region watermark insertion and genetic algorithm-based watermark extraction are possible in the algorithm. Ziqiang and coauthors integrated DWT with Particle Swarm Optimization (PSO) for watermarking digital images. The technique embeds watermark into coefficients of DMT that holds value larger than some threshold value. Subsequently the extraction is performed through PSO. However, an obvious limitation of their proposed method is that the application of PSO was simply done for evaluating the feasibility of the extracted watermarks.

Research objective: The aim of this research is to acquire accomplishing maximum robustness and transparency into consideration in transform domain that preserve the intellectual property of images and it will be verified with the samples. The objectives of this research are to:

- Design an enhanced algorithm for embedding and extracting the watermark code inside images using wavelet based watermarking method
- Evaluate the performance of the proposed algorithm by comparing it with existing works by calculating the PSNR value
- Validate the robustness of the algorithm by using common attacking techniques

Scope of the research: Research activities in digital image watermarking have become more specialized. Therefore, it is important to identify the focus of study. In this study, we investigate robust, semi-fragile watermarking and hybrid methods. In addition, we also examine hybrid methods that combine the advantages of robust and semi-fragile watermarks.

To preserve the visual appearance of images, we focus on invisible watermarks. The experiments are performed using grey scale images so as to focus on the fundamentals of data embedding. The developed watermarking methods can be easily ported to colour images given the similar pixel representation of both greyscale and colour images. In this study, we introduce a novel algorithmic framework for solving an embedding and extracting problem. The optimal algorithm achieves this by using a forecasted feasibility for parameters evaluation in discrete wavelet transform domain. We also need to consider trade-off between watermark properties that have conflicting characteristics, i.e., robustness, capacity and imperceptibility. We also emphasized the computational efficiency of the algorithms.

MATERIALS AND METHODS

Now-a-days, researchers are focusing on mixing of spatial and transformed domains (i.e., combinations of DFT, DWT and DCT) concepts and also applying more and more mathematical and statistical model and other interdisciplinary approaches in watermarking: for example use of chaotic theory, fractal image coding, etc. In this section we are presenting the brief of few recent watermarking algorithms.

Cox *et al*. (2001), researcher presented a reversible watermarking scheme for the 2D-vector data (point coordinates) which are used in geographical information related applications. This reversible watermarking scheme exploits the high correlation among points in the same polygon in a map and achieves the reversibility of the whole scheme by an 8-point integer DCT which ensures that the original 2D-vector data can be watermarked during the watermark embedding process and then perfectly restored during the watermark extraction process. In this scheme, reseacher used an efficient highest frequency coefficient modification technique in the integer DCT domain to modulate the watermark bit "0" or "1" which can be determined during extraction without using any additional information. To alleviate the visual distortion in the watermarked map caused by the coefficient modification, they proposed an improved reversible watermarking scheme based on the original coefficient modification technique. They serve as building blocks for the zero-knowledge implementation of the generalized Gaussian ML detector and also open new possibilities in the design of high level protocols.

RESULTS AND DISCUSSION

Researchers have proposed a framework research methodology as shown in Fig. 1. The framework consists of four phases such as initial phase, preprocessing phase, construction phase and improvement phase. The phases are described as following.

Testing phase: In this phase the proposed approaches will be tested on the copy of the certificates that issued from/to ministry of higher education in Iraq to avoid forgery.

Initial phase: This phase includes studying of the current state of art in the watermarking research and the applications that can support getting an idea in the watermarking the images.

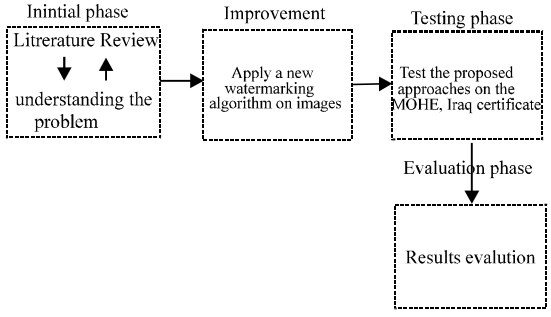

Fig. 1: Flowchart of research program

Improvement phase: In this phase new watermarking approaches will be applied on some images to handle to forgery certificates problem.

Evaluation phase: In this phase the proposed approaches will be evaluated based on criteria for watermarking.

CONCLUSION

Based on detailed literature review, research implications of some of the application areas like fingerprinting and copyright protection are very high and till now no successful algorithm seems to be available to prevent illegal copying of the multimedia contents, the primary goal of this study work is to develop watermarking schemes for images (which are stored in spatial domain as well as transformed domain) which can sustain the known attacks and various image manipulation operations. Out of image, audio and video, the image watermarking was chosen as a goal because any successful image watermarking algorithm may be extended to video watermarking also. Therefore, to keep the future extension in mind, the cover medium chosen is an image.

REFERENCES

Ahmidi, N. and R. Safabakhsh, 2004. A novel DCT-based approach for secure color image watermarking. Proceedings of the International Conference on Information Technology: Coding and Computing, Volume 2, April 5-7, 2004, Tehran, Iran, pp: 709-713.

Arnold, M., M. Schmucker and S.D. Wolthusen, 2003. Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Inc., Norwood, MA.

Barni, M., F. Bartolini, V. Cappellini and A. Piva, 1998. A DCT-domain system for robust image water marking. Signal Process., 66: 357-372.

Barni, M., F. Bartolini, V. Cappellini, A. Lippi and A. Piva, 1999. A DWT-based technique forspatio-frequency masking of digital signatures. Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents, Volume 3657, January 25-27, 1999, San Jose, CA., pp: 31-39.

Cox, I.J., M. Miller and J. Bloom, 2001. Digital Watermarking: Principles and Practice. Morgan Kaufmann, Burlington.

Lee, G.J., E.J. Yoon and K.Y. Yoo, 2008. A new LSB based digital watermarking scheme with random mapping function. Proceedings of the International Symposium on Ubiquitous Multimedia Computing, October 13-15, 2008, Hobart, ACT., pp: 130-134.