

Chapter 58

On the Implementation of a Digital Image Watermarking Framework Using Saliency and Phase Congruency

Abhishek Basu

RCC Institute of Information Technology, India

Susmita Talukdar

Infosys Ltd., India

ABSTRACT

In this paper, a saliency and phase congruency based digital image watermarking scheme has been projected. The planned technique implants data at least significant bits (LSBs) by means of adaptive replacement. Here more information is embedded into less perceptible areas within the original image determined by a combination of spectral residual saliency map and phase congruency map. The position of pixels with less perceptibility denotes the most unimportant region for data hiding from the point of visibility within an image. Therefore any modification within these regions will be less perceptible to one observer. The model gives a concept of the areas which has excellent data hiding capacity within an image. Superiority of the algorithm is tested through imperceptibility, robustness, along with data hiding capacity.

INTRODUCTION

Digital domain provides various advantages like noise immunity, flexibility of implementation, easy data storage, low power consumption, scalability etc. over analog domain, as published by Pelgrom (2010). However all the natural signals are analog, digitization is required for processing by means of sampling and quantization. Though due to quantization some information loss occurs in the form of quantization error but this error can be minimized by altering the number of quantization levels as per Freeman (2005). In addition to that signal processing is simpler and more reliable in digital domain with lower

DOI: 10.4018/978-1-5225-5204-8.ch058

cost. As a result technology switches over to digital domain, according to Proakis (2007) and Salivahanan and Gnanapriya (2011). This technology swap creates a revolution in information technology and data transmission over digital channels or in World Wide Web as published by Wolinsky Art (1999). Over and above the immense advantages offered by the Digital domain creates a boom in digital systems by means of digital consumer devices, according to the publication of Dhir (2004)

The enormous popularity of internet along with digital consumer devices like digital cameras, scanners etc, has become an indispensable part of people's live. At the same time as the popularity increases, access and storage of digital information become very easier. Accordingly a budding quantity of personal information about the users in addition to other digital data is stored in electronic form and that is generally transferred using unrestricted electronic means, as published by Fegghi Jalal et al. (1999). This effortless accessibility of digital information and the simplicity of the digital systems have left the contents over the digital media extremely insecure, in reference with Bidgoli Hossein (2006) and Furht Borko and Kirovski Darko (2006). This shows the way to the emerging problems like Copyright Protection as proposed by Farhadzadeh and Voloshynovskiy (2014), Nasir et al. (2007), Gertz Michael & Jajodia Sushil (2007) Wu Zhijun, (2014) and Zhang D et al (2009), Authenticity in print by Dal Park Geum et al. (2007), Eswaraiiah R. & Reddy E.S., (2014), Otum Hazem Munawer Al (2014) & Wu Yongdong (2006), integrity verification and security of the digital information as proposed by Hosmer Chet, (2002), Li Chang-Tsun et al. (2010), Lynch C., (2000) & White paper, Digimarc Corporation (2004). As a result, the need for mechanisms to protect such information is undeniable.

Digital edition of information possesses intrinsic advantages of portability; efficiency and accuracy of information content, but alternatively, this production also place a severe intimidation of perfect and illegal replica in unlimited number as mentioned by Bandyopadhyay M. N., (2005), Horowitz Paul & Hill Winfield, (1989) & Pohlmann Ken C., (1992). To solve this challenging problem on the subject of data transmission in network surrounding, information hiding came as an efficient solution. Protecting copyright has initiated research to discover ways to hide copyright information or serial into digital data; the second one can help to identify copyright infringement, and the first one to take legal action as published by Anderson R., (1996), Wayner Peter, (2009) & Wei Chang Bao, (2014). Information hiding is a prospective means for copyright protection, authentication and integrity verification as well as intellectual property right protection as proposed by Kang X, Wei S., (2008) & Lo ChunChin et al. (2014).

Information hiding ensures the safety of data from corruption and helps to ensure privacy as well as secure communication. Now the idea of secret communication is very old, from ancient age people are trying to maintain the secrecy of message as mentioned in Janeczko Paul B., (2006), Jung Ki-Hyun, Yoo Kee-Young, (2014) & Kahn David, (1996). Starting since Homer's Iliad, stories by Herodotus, Kautilya's Arthashastra, Vatsayana's Kamasutra etc. the concealment of message is one of the important task worldwide in different era as mentioned in Herodotus, (1972), Homer, (1972) & Kautilya, (1992).

Information hiding can be classified as:

Steganography

Steganography is the process of writing message in such an ambiguous way that only sender and receptor can figure out the existence of the message as printed in Aura, T. (1996), Craver, S. (1997) & Simmons, G. J. (1984). The word steganography is of Greek origin and means "concealed writing" appeared from the Greek words "steganos" which stands for "covered or protected", and "graphein" meaning "to write" as per Johannes Trithemius, (1606). The advantage of steganography, over cryptography is that it protects

38 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/on-the-implementation-of-a-digital-image-watermarking-framework-using-saliency-and-phase-congruency/197007

Related Content

Shape Retrieval and Classification Based on Geodesic Paths in Skeleton Graphs

Xiang Bai, Chunyuan Li, Xingwei Yang and Longin Jan Latecki (2013). *Graph-Based Methods in Computer Vision: Developments and Applications* (pp. 190-215).

www.irma-international.org/chapter/shape-retrieval-classification-based-geodesic/69077

A Compilation of Methods and Datasets for Group and Crowd Action Recognition

Luis Felipe Borja, Jorge Azorin-Lopez and Marcelo Saval-Calvo (2017). *International Journal of Computer Vision and Image Processing* (pp. 40-53).

www.irma-international.org/article/a-compilation-of-methods-and-datasets-for-group-and-crowd-action-recognition/188760

A Reflexion on Implementation Version for Active Appearance Model

Oum El Kheir Naoui, Ghalem Belalemand Saïd Mahmoudi (2013). *International Journal of Computer Vision and Image Processing* (pp. 16-30).

www.irma-international.org/article/a-reflexion-on-implementation-version-for-active-appearance-model/95968

Machine Vision Optical Scanners for Landslide Monitoring

Javier Rivera Castillo, Moises Rivas-Lopez, Wendy Flores-Fuentes, Oleg Sergiyenko, Julio Cesar Rodríguez-Quíñonez and Daniel Hernandez-Balbuena (2017). *Developing and Applying Optoelectronics in Machine Vision* (pp. 206-235).

www.irma-international.org/chapter/machine-vision-optical-scanners-for-landslide-monitoring/161992

A Review on Chaos-Based Image Encryption Using Fractal Function

Anandkumar R. and Kalpana R. (2020). *Examining Fractal Image Processing and Analysis* (pp. 23-37).

www.irma-international.org/chapter/a-review-on-chaos-based-image-encryption-using-fractal-function/236820