RESILIENCE OF DIGITAL WATERMARKS UNDER TRANSFORMATION ATTACKS

Srilal Buddika T.M.

Registration No. : 138204V

Degree of Master of Science

Department of Computer Science & Engineering

University of Moratuwa

Sri Lanka

April 2015

RESILIENCE OF DIGITAL WATERMARKS UNDER TRANSFORMATION ATTACKS

Srilal Buddika T.M.

Registration No. : 138204V

Dissertation submitted in partial fulfillment of the requirements for the degree Master of Science in Computer Science

Department of Computer Science & Engineering

University of Moratuwa

Sri Lanka

April 2015

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Candidate

....

Date *T.M.S. Buddika*

The above candidate has carried out research for the Masters Dissertation under my supervision.

Supervisor

....

Date *Dr. Chandana Gamage*

Acknowledgments

I offer my sincerest gratitude to my research supervisor Dr. Chandana Gamage, who gave endless support and encouragement to me during the research work and thesis preparation. His supervision has always inspired me to improve my writing skills and to produce quality work on this thesis.

I would like to extend my gratitude to my wife and family for providing assistance, support, encouragement and inspiration during the writing of this dissertation. I greatly appreciate their support and commitment in making this thesis a success.

Abstract

Digital watermarking of electronic data has become a popular research area over last several years. The research work presented in this thesis blends a more practical perspective of digital watermarking schemes against transformation/geometric attacks with theoretical studies presented in past literature. Main objective of this dissertation is to come up with an attack success/failure evaluation metric against chosen watermarking schemes and with set of attacks. "Success" or "Failure" is defined as per given criteria: If there is a legitimate owner for the image, *success* of image attack would be determined if recovery of the watermark is denied given the fact that attacked image lies within the perceptual range. Otherwise it would be depicted as a *failure* of image attack.

In this thesis, limits that preserve perceptual quality of subjected images were analyzed for different types of attacks. Both PSNR and Histogram Analysis provide a foundation for meaningful measurement. We have shown that coupling such measurements with a perceptual quality measurement provide meaningful values for effectiveness of a watermarking scheme.

Table of Contents

List of Figures

List of Tables

List of Equations