AIN SHAMS UNIVERSITY
Faculty of Computer and
Information Sciences
Computer Science Department

Developing an adaptive algorithm for information hiding in video streams

Thesis submitted to the Department of Computer Science
Faculty of Computer and Information Sciences
Ain Shams University

In partial fulfillment of the requirements for the degree
Of Master in Computer and Information Sciences

By

Mennatallah Mostafa Sadek Hassan

B.Sc. in Computer and Information Sciences (2009)
Ain Shams University – Cairo

Under the supervision of

Prof. Dr. *Mostafa Gadal-Haqq M. Mostafa*

Professor of Computer Science
Faculty of Computer and Information Sciences
Ain Shams University

Dr. Amal Said Mohammed Khalifa
Assistant Professor, Scientific Computing Department
Faculty of Computer and Information Sciences
Ain Shams University
Cairo-2015

To my dear parents

To my beloved husband

Acknowledgements

I acknowledge my deep gratitude to ALLAH for providing me with the strength to complete this work on a level that I hope will please the reader.

I wish to express my sincere and heartfelt appreciation to my supervisor; Prof. Mostafa Gadal-Haqq for his supervision, resourceful ideas and suggestions that helped in enhancing my work.

Special thanks are due to my supervisor Dr. Amal Said Khalifa for her continuous guidance and encouragement in achieving this work.

Without their assistance and dedicated involvement in every step throughout the process, this thesis would have never been accomplished. I would like to thank you very much for your support and understanding.

Finally, with all my appreciation and love that no words can describe, my deepest gratitude goes to my family for their love, prayers and endless support; my dear parents and my loving husband who supported me and endured a lot to lead me to success in my life and my career!

Abstract

Steganography is the art and science of secret communication. Modern cover types can take different forms. Nowadays, video streams are transmitted more frequently on internet websites imposing a larger practical significance on video steganography. A video can be considered a sequence of images. Information hiding in video has a variety of techniques. Although great efforts were done in developing these techniques, but most of them suffer from intolerance to video processing attacks and lack any intelligent processing of the cover video.

Adaptive video steganography was recently proposed in the literature. It aims to achieve better quality of the stego-video by intelligently processing the cover according to some criteria. This helps to identify the best regions for data hiding, referred to as Regions Of Interest (ROI). A recent research by Cheddad et al. showed that data embedding in human skin regions as ROI yield better imperceptibility and increase the hiding robustness.

In this work, a blind adaptive algorithm for robust video steganography is proposed. The proposed algorithm adaptively processes the cover video and hides data in its human skin regions. A skin map is created for each frame using a fast adaptive skin detection method. Then a blocking step is applied on the produced skin-map converting it into a skin-block-map for discarding the error-prone skin pixels and enhancing the extraction quality. Next, the skin-block-map is used for guiding the embedding procedure. Finally, the secret bits are embedded in the detail coefficients of the red and blue components of each frame using a wavelet quantization-based algorithm for achieving robustness against MPEG-4 compression. Hiding capacity, imperceptibility, extraction accuracy and robustness against MPEG-4 compression of the proposed algorithm were tested. Results show the high imperceptibility of the proposed algorithm and its robustness against MPEG-4 compression.

List of Publications

- Mennatallah M. Sadek, Amal S. Khalifa, and Mostafa GM Mostafa. "Video steganography: a comprehensive review." *Multimedia Tools and Applications.* vol.74 no.17 pp: 7063-7094, 2014. doi: 10.1007/s11042-014-1952-z .

- Mennatallah M. Sadek, Mostafa G. M. Mostafa, and Amal S. Khalifa. "A skin-tone block-map algorithm for efficient image steganography." *9th International Conference on Informatics and Systems (INFOS),* 15-17 December, pp: DEKM-27, 2014. IEEE.

- Mennatallah M. Sadek, Amal S. Khalifa and Mostafa G. M. Mostafa. "Robust Video Steganography Algorithm Using Adaptive Skin-tone Detection". *Multimedia Tools and Applications*, December 2015.

Table of Contents

List of Figures.....vi

List of Tables.....ix

Chapter 1 Introduction.....2

1.1. Overview.....2

1.2. Motivation.....3

1.3. Problem Statement.....4

1.4. Research Objectives.....4

1.5. Proposed Work.....5

1.6. Thesis Organization.....5

Chapter 2 Background.....8

2.1. Cryptography, Steganography and Watermarking.....8

2.2. Steganography Types.....10

2.3. Video File Formats.....12

2.4. Video Compression.....13

2.5. Color Spaces.....18

2.6. Image Transforms.....21

2.6.1. Discrete Fourier Transform.....21

2.6.2. Discrete Cosine Transform.....22

2.6.3. Discrete Wavelet Transform.....23

Chapter 3 Video Steganography.....27

3.1. Overview.....27

3.2. Substitution-based Techniques.....29

3.3. Transform Domain Techniques.....34

3.4. Adaptive Techniques.....38

3.5. Format-based Techniques.....40

3.6. Cover Generation Techniques.....42

3.7. Summary.....51

Chapter 4 Skin Tone Detection.....54

4.1. Skin Detection Overview.....54

4.2. Skin Detection Methods.....55

4.3. Skin Detection Results.....59

4.4. Summary.....63

Chapter 5 Adaptive Skin-tone Video Steganography 66

5.1. Overview of the proposed work 66

5.2. Skin-block-map Generation 68

5.2.1. Skin-map Generation 68

5.2.2. Skin-map Blocking 68

5.3. Wavelet Quantization-Based Hiding 69

5.4. Wavelet Quantization-Based Extraction 73

5.5. Summary 75

Chapter 6 Results and Discussions 78

6.1. Performance Measures 78

6.2. Test Data Sets 79

6.3. Image Results 80

6.4. Video Results 84

6.4.1. Skin-map Blocking Effect 84

6.4.2. Parameter Tuning 86

6.4.2.1. Color Space Selection 86

6.4.2.2. Block Size Selection 88

6.4.3. Comparison with Other Approaches 91

Chapter 7 Conclusion and Future Work 94

7.1. Summary of the work 94

7.2. Conclusion 95

7.3. Future Work 96

Appendix A: Skin Detection 97

Appendix B: Adaptive Skin-tone Video Embedding 100

Appendix C: Adaptive Skin-tone Video Extraction 103

References 105

List of Figures

Figure 1.1 General steganography model. 2

Figure 2.1 General cryptographic system. 8

Figure 2.2 Types of steganography according to the cover. 11

Figure 2.3 Video file format. 13

Figure 2.4 Systems involved in video compression. 14

Figure 2.5 Components of a video encoder 15

Figure 2.6 Video encoding process. 15

Figure 2.7 I, P and B frames arranged inside a GOP [38]. 16

Figure 2.8 Hierarchy of MPEG video file [39]. 17

Figure 2.9 (a) Sample video frame decomposed into (b) Red, (c) Green and (d) Blue channels. 18

Figure 2.10 RGB color space visualized as a cube [41]. 18

Figure 2.11 Additive color composition of the RGB color space [41]. 19

Figure 2.12 (a) Sample video frame decomposed into (b) Luma (Y), (c) Chromatic blue (Cb) and (d) Chromatic red (Cr) channels. 20

Figure 2.13 Cylindrical coordinates of (a) HSL color space (b) HSV color space [43]. 21

Figure 2.14 (a) Original image (b) 1-level 2D DWT decomposition (c) 2-level 2D DWT decomposition. 24

Figure 3.1 (a), (b), (c) Various classifications of steganography methods. 28

Figure 3.2 Adopted classification for steganography methods. 29

Figure 3.3 (a) First frame of the cover video before embedding (b) Secret image (http://ragreen007.blogspot.com/). 29

Figure 3.4 Resultant stego-frames using 1 to 5 least significant bits for hiding.30

Figure 3.5 (a) Original image (b) Resultant grid from partitioning overlaid on the original image [67]. 31

Figure 3.6 (a) Noise-like region. (b) Informative region [63]. 33

Figure 3.7 Hiding process for [59]. 35

Figure 3.8 Detailed hiding steps for [58]. 36

Figure 3.9 Adaptive LSB [77] embedding process. 39

Figure 3.10 H.264 data hiding algorithm for [80]. 41

Figure 3.11 Dynamic cover generation method: inputs and pre-processing [83]. 43

Figure 4.1 Density plot of Asian, African, and Caucasian skin in different color spaces [85]. 55

Figure 4.2 Asian, African and Caucasian skin clusters in co-locate in the CbCr space [85]. 58

Figure 4.3 Framework for Khan et al. [93] skin detection algorithm. 58

Figure 4.4 Test image, Khan et al. [93] skin-map and Cheddad et al. [8] skin-map. 60

Figure 4.5 First video frame, Khan et al.[93] skin-map, Cheddad et al. [8] skin-map. 61

Figure 4.6 Skin detection runtime for each of the five test images using Khan et al. [93] algorithm and Cheddad et al. [8] algorithm. 62

Figure 4.7 Skin detection runtime for the first frame of each test video using Khan et al. [93] algorithm and Cheddad et al. [8] algorithm. 63

Figure 5.1 System architecture of the proposed method. 67

Figure 5.2 2x2 Skin map blocking example. 69

Figure 5.3 Detailed example of Khalifa et al. [9] wavelet quantization-based data hiding process. 70

Figure 5.4 Detailed steps of the proposed data embedding process. 71

Figure 5.5 Detailed steps of the extraction process of the proposed method. 73

Figure 5.6 Detailed example of Khalifa et al. [9] wavelet quantization-based data extraction process. 74

Figure 6.1 (a – e) Set of test images used for image experimental results and (f) Chosen secret message. 79

Figure 6.2 Set of test video sequences used for experimental results (a) Suzie (b) Foreman (c) Advertisement (d) Salesman (e) Car phone and (f) Chosen secret message. 80

Figure 6.3 Skin-maps for “waving girl” image (a)skin-map with no blocking, (b) with 2x2 blocking (c) with 4x4 blocking (c) with 8x8 blocking.................81

Figure 6.4 Stego-images for each test image produced using 2x2, 4x4 and 8x8 block sizes respectively...83

Figure 6.5 Skin-maps for 1st frame of Foreman video (a)skin-map with no blocking, (b) with 2x2 blocking (c) with 4x4 blocking (c) with 8x8 blocking. .85

Figure 6.6 Number of different pixels between embedding and extraction skin-block-maps for the first 15 frames of advertisement video. 86

Figure 6.7 First stego-frame for each test video produced using 2x2, 4x4 and 8x8 block sizes respectively. 90

List of Tables

Table 2.1 Comparison between cryptography, steganography and watermarking technologies. 10

Table 2.2 Comparison between Intra-frame and Inter-frame encoding. 17

Table 2.3 Transformation from RGB to orthogonal color spaces. 20

Table 3.1 Pros, cons and embedding capacity of the discussed techniques. 44

Table 6.1 Proposed method performance under various block sizes for ‘Waving girl’, ‘Mandy’ and ‘Smiling people’ images. 82

Table 6.2 Proposed method performance under various block sizes for ‘Smiling children’ and ‘Family images. 82

Table 6.3 Comparison of robustness against JPEG compression with Cheddad et al. [8] method. 84

Table 6.4: Performance of the proposed method in YCbCr colorspace. 87

Table 6.5: Performance of the proposed method in RGB colorspace. 87

Table 6.6: Proposed method performance under various block sizes for Suzie, Foreman and Advertisement videos. 88

Table 6.7: Proposed method performance under various block sizes for Salesman and Car phone videos. 88

Table 6.8: Comparison of performance with other approaches. 91

Table 6.9: Comparison of robustness against MPEG-4 compression with Cheddad et al. [8] method 92

Chapter 1

Introduction

1.1 Overview

1.2 Motivation

1.3 Problem Statement

1.4 Research Objectives

1.5 Proposed Work

1.6 Thesis Organization

Chapter 1

Introduction

1.1.Overview

The revolution in digital information has created new challenges for sending a message in a safe and secure way. Whatever method is chosen, the most important question is its degree of security. Numerous approaches have been developed for addressing the issue of information security such as cryptography, steganography and watermarking.

Steganography is the art and science of invisible communication. The origin of the word steganography comes from the Greek language. It is derived from two Greek words "*stegos*" which means "cover" and "*grafia*" which means "writing" [1]. Steganography evolved driven by the need to hide the existence of a secret communication.

Steganography has some common terminology. The term *cover object* describes the file used for hiding information. The *secret message* refers to the data that is embedded in the cover through an embedding module. A *stego-object* is produced combining the cover object with the embedded data. In case of encrypting the secret message before embedding, an encryption key is used. This key is referred to as *stego-key*. Furthermore, the term *steganalysis* refers to the different attacks that try to break the steganographic algorithm. Figure 1.1 shows a general steganographic model. Embedding process is represented with bold arrows, while extraction process is represented with non-bold arrows.

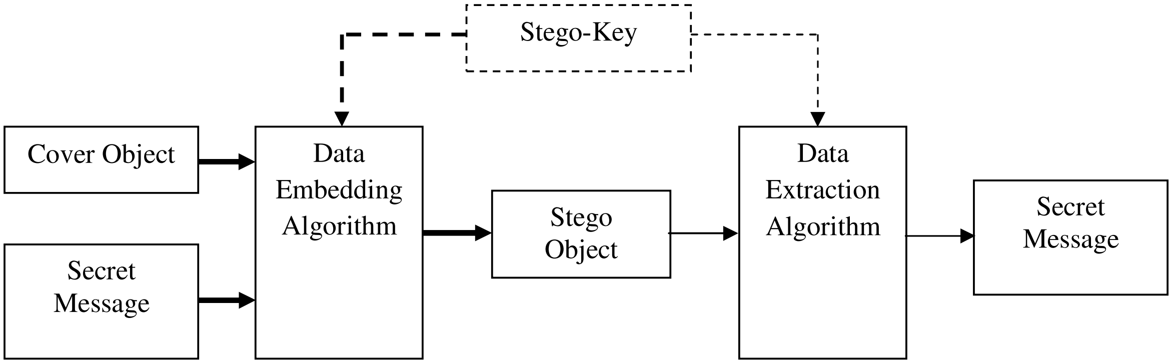

Figure 1.1 General steganography model.

However, designing a good steganography algorithm is not a trivial task. It requires achieving robustness, tamper resistance, high hiding capacity and perceptual transparency. The challenge lies in the fact that these four aspects are inversely proportional to each other creating the data hiding dilemma. Robustness is the amount of modification the stego-object could withstand before an adversary destroys the hidden information [2]. Tamper resistance is the difficulty for an attacker to change the secret message after it has been embedded in the cover object. On the other hand, there is a trade-off between the hiding capacity and the perceptual transparency. When the hiding capacity increases, a smaller cover object could be used for hiding the secret message. This results in a stego-object with a smaller size that can be easily transmitted over the internet. But increasing the hiding capacity leads to visual distortions in the stego-object. If an attacker detects the distortion, then the presence of the hidden message is revealed and steganography is considered failed. To avoid such a situation, an appropriate cover file should be chosen carefully.

1.2.Motivation

Since a substantial amount has already been invested in the development of the software and hardware infrastructure for standard data transmission, it makes monetary sense to use the same infrastructure for transmission of secure or non-standard data. This can be achieved by embedding the secret data in an innocent-looking cover file using steganography. Almost any digital file can be used as a cover.

Although images are still the most used type of cover files due to their popularity on the internet, recently, video streams have gained practical significance due to the huge advancement of the multimedia technology. A video is considered a sequence of images (frames). Usually, a video have a large number of frames. For example a 5 minutes video playing at a frame rate of 30 frames per second has 9,000 frames. This constitutes a quite large amount of redundant data that is perfectly suitable for steganography. A lot of image steganographic techniques can be extended to videos as well [3-5].

Numerous video steganographic techniques were proposed in the literature, but most of these techniques suffer from several issues:

- Some techniques work on uncompressed videos. This makes most of them not robust to compression.
- On the other hand, techniques working on compressed videos may require partial or full decompression of the video.
- Lack of intelligent video processing. That is, all video frames are equally utilized in the hiding process without following any adaptive approach.
- The whole frame is involved in the hiding process which affects the visual quality of the resultant stego-file.

1.3.Problem Statement

Although great efforts were recently invested in developing video steganography techniques, most of them suffer from intolerance to video compression. According to [6] one of the solutions for increasing robustness lies in identifying certain regions of interest in the cover that can be used for hiding. They proposed using human skin regions for this purpose. In an earlier work [7], data hiding in human skin regions of images was proved to be robust to compression.

Steganography in human skin regions involves adaptively processing the cover video frames and applying computer vision techniques for detection of human skin regions. This limits the focus of the embedding scheme to only Regions-Of-Interest (ROI). Recent research showed that embedding data in ROI not only increases the hiding robustness, but also yields better imperceptibility [8].

1.4.Research Objectives

The objective of this thesis can be summarized in the following points:

- Comprehensive study of the state of the art of video steganography techniques.
- Developing an adaptive technique for video steganography based on skin tone detection.
- Evaluating the performance of the proposed technique in comparison with other methods in the literature.