**MEDI-CAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENT, INDORE**



A Major Project

Submitted in partial fulfillment of the requirement for the award of Degree of

**Bachelor of Engineering in Electronics and Communication**

**CRYPTOGRAPHY USING SELECTIVE ENCRYPTION**

Submitted by

**Abhinav Jha (0812EC141007)**

**Akshanshi Jain (0812EC141016)**

**Akshita Pathak (0812EC141019)**

**Aman Thakur (0812EC141025)**

**Electronics and Communication Engineering Department**

**MEDI-CAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENTINDORE- 453331**

**2017-2018**

**MEDI-CAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENT, INDORE**



A Major Project

Submitted in partial fulfillment of the requirement for the award of Degree of

**Bachelor of Engineering in Electronics and Communication**

**CRYPTOGRAPHY USING SELECTIVE ENCRYPTION**

Guided by: MR. HARIOM PATIDAR

Project Coordinator: MR. ANKIT SAXENA

**Electronics and Communication Engineering Department**

**MEDI-CAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENT INDORE- 453331**

**2017-2018**

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING MEDICAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENT, INDORE (M.P.)**



# CERTIFICATE

The dissertation entitled **CRYPTOGRAPHY USING SELECTIVE ENCRYPTION** being submitted by **Abhinav Jha (0812EC141007), Akshanshi Jain (0812EC141016), Akshita Pathak (0812EC141019)** and **Aman Thakur (0812EC141025)** has been examined by us and is hereby approved for the EC 805 Major Project, for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, the opinion expressed or conclusion drawn therein, but approve the dissertation only for the purpose for which it has been submitted.

Mr. Ankit Saxena Mr. Hariom Patidar

(Project Coordinator) (Project Guide)

Date: Date:

Mr. Ajay Kulkarni

(Head of Department)

Date:

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING MEDICAPS INSTITUTE OF TECHNOLOGY AND MANAGEMENT, INDORE (M.P.)**



# CERTIFICATE OF APPROVAL

The dissertation entitled **CRYPTOGRAPHY USING SELECTIVE ENCRYPTION** being submitted by **Abhinav Jha (0812EC141007), Akshanshi Jain (0812EC141016), Akshita Pathak (0812EC141019)** and **Aman Thakur (0812EC141025)** has been examined by us and is hereby approved for the EC805 Major Project, for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, the opinion expressed or conclusion drawn therein, but approve the dissertation only for the purpose for which it has been submitted.

(Internal Examiner) (External Examiner)

Date: Date:

# ACKNOWLEDGEMENT

We would like to articulate our deep gratitude to our project guide Prof.Hariom Patidar and our project coordinator Prof.Ankit Saxena who has always been our motivation for carrying out the project. It is our pleasure to refer MATLAB software and Microsoft Office exclusive of which the compilation of this report would have been impossible. An assemblage of this nature could never have been attempted without reference to and inspiration from the works of others whose details are mentioned in reference section. We acknowledge out indebtedness to all of them.Last but not the least, our sincere thanks to all of our friends who have patiently extended all sorts of help for accomplishing this undertaking.

Abhinav Jha (0812EC141007)

Akshanshi Jain (0812EC141016)

Akshita Pathak (0812EC141019)

Aman Thakur (0812EC141025)

# ABSTRACT

This project proposed the scheme for Cryptography (separable reversible data hiding technique in an encrypted image) using Selective Encryption algorithm. In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys.

In this project the original image was encrypted using an encryption key. Then, a data-hider hides the data using data-hiding key to provide an additional security. With an encrypted image containing additional data, if a receiver has the data-hiding key, it can extract the additional data though it does not know the image content and if it has the encryption key, it can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the key it can extract the additional data and recover the original content without any error. This results in security of image and data.

# Table of Content

[CERTIFICATE ii](#_Toc511849569)

[CERTIFICATE OF APPROVAL iii](#_Toc511849570)

[ACKNOWLEDGEMENT iv](#_Toc511849571)

[ABSTRACT v](#_Toc511849572)

[Table of Content 2](#_Toc511849573)

[List of Figures 5](#_Toc511849574)

[List of tables 6](#_Toc511849575)

[CHAPTER 1 7](#_Toc511849576)

[1.1.Introduction 7](#_Toc511849577)

[1.2.Motivation 8](#_Toc511849578)

[1.3.Objective 8](#_Toc511849579)

[1.4.Thesis Outline 9](#_Toc511849580)

[CHAPTER 2 10](#_Toc511849581)

[2.1. Literature Survey 10](#_Toc511849584)

[2.2.Tool/Platform Detail 11](#_Toc511849585)

[CHAPTER 3 13](#_Toc511849586)

[3.1.Problem Description 13](#_Toc511849588)

[3.2.Proposed Solution 13](#_Toc511849589)

[3.2.1.Selective Encryption 14](#_Toc511849590)

[3.3.Design – Steps 17](#_Toc511849591)

[3.4.Implementation-Logic Description 18](#_Toc511849592)

[3.5. Methodology 20](#_Toc511849593)

[CHA PTER 4 22](#_Toc511849594)

[4.1.Milestones 22](#_Toc511849595)

[4.2 Individual and Team work report 23](#_Toc511849596)

[chapter 5 24](#_Toc511849598)

[RESULT 24](#_Toc511849599)

[CHAPTER 6 26](#_Toc511849600)

[6.1.Conclusion and Future Scope 26](#_Toc511849602)

# List of Figures

[Figure 1 Encryption of image 14](#_Toc511776088)

[Figure 2 Selective encryption mechanism 15](#_Toc511776089)

[Figure 3 Flowchart Planning 16](#_Toc511776090)

[Figure 4 Separable reversible data hiding in an encrypted image 18](#_Toc511776091)

[Figure 5 Output at the sender’s side 23](#_Toc511776092)

[Figure 6 Output at the receiver's side 24](#_Toc511776093)

# List of tables

[Table 1 Individual Report 18](#_Toc511776008)

# CHAPTER 1

## Introduction

Cryptography involves creating written or generated codes that allows information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without anyone decoding it back into a readable format, thus compromising the data. There are two basic types of cryptography or encryption schemes: Symmetric-key and public-key encryption.In symmetric-key schemes, the encryption and decryption keys are the same. Thus, communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages.Public-key encryption is a relatively recent invention, historically, all encryption schemes have been symmetric-key (also called private-key) schemes. This project focuses on separable reversible data hiding which will result in security of both the data and image independently. Encryption has long been used by militaries and governments to facilitate secret communication.It is now commonly used in protecting information within many kinds of civilian systems.For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage.Encryption can be used to protect data "at rest", such as files on computers and storage devices (e.g. USB flash drives).In recent years there have been numerous reports of confidential data such as customers' personal records being exposed through loss or theft of laptops or backup drives.Encrypting such files at rest helps protect them should physical security measures fail.Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection) is another somewhat different example of using encryption on data at rest.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

## Motivation

Since times immemorial, security of data to maintain its confidentiality, proper access control, integrity and availability has been a major issue in data communication. Today images and data transfer in mobile phone communication, e-commerce, Pay-TV, sending private e-mails, transmitting financial information and touches on many aspects of daily lives. We wanted to develop a scheme in which the data embedded in an image and the image itself would be secured from any unauthorized access. This scheme would also be a merit in military and medical services.

## Objective

Objective of this project is to build an efficient cryptography technique so as to provide security to the sent images and data. This security will be provided via encryption keys which will be different for data and image providing dual security. The receiver will only be able to access the data and image if the decryption key matches the original key.

## Thesis Outline

The brief outline of the covered chapters in this document is highlighted below:

CHAPTER 2: This chapter includes the Literature Survey on Cryptography and Separable Reversible Data Hiding in an embedded image from various sources and earlier published work. This chapter also includes the description about the platform/tool on which the project is based.

CHAPTER 3: This chapter includes the description of the problems related to the topic and proposed solution to overcome the earlier drawbacks of the system.

CHAPTER 4: This chapter highlights the design steps that have to be followed for the accomplishment of the project and to get desired outputs. This chapter also gives the description of proposed method.

CHAPTER 5:This chapter describes the methodology included in this project.

CHAPTER 6**:** The results achieved are displayed/ attached in this section.

CHAPTER 7:This chapter includes the conclusion and future scope related to the project.

# CHAPTER 2



## 2.1. Literature Survey

In [5] authors described that data hiding emphases on the data embedding/extracting on the plain spatial domain. But, in some scenarios, a media assistant or a channel administrator hopes to append some additional message, such as the origin, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content (payload) should be recovered without any error after image decryption and message extraction at receiver side. In [8] the authors presented that a content owner encrypts the original image using an encryption key, and a data-hide embeds additional data into the encrypted image using a data hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In [7] the scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data.

## 2.2. Tool/Platform Detail

SOFTWARE REQUIREMENT:

1. Operating System- Windows

2. MATLAB

There are several Open Source option for numerical computing tht runs across all major platforms like Windows, Mac etc namely

a) GNU Octave

b) Scilab

c) Sage

d) Matlab

In this project the platform used is MATLAB. The name MATLAB stands for matrix laboratory. MATLAB was originally written to provide easy access to matrix software developed by the LINPACK and EISPACK projects, which together represent the state-of-the-art in software for matrix computation. MATLAB has evolved over a period of years with input from many users. In university environments, it is the standard instructional tool for introductory and advanced courses in mathematics, engineering, and science. In industry, MATLAB is the tool of choice for high-productivity research, development, and analysis MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

Typical uses of Matlab include:

* Math and computation
* Algorithm development
* Modeling, simulation, and prototyping
* Data analysis, exploration, and visualization
* Mathematical functions for linear algebra, statistics, Fourier analysis, filtering, optimization, and numerical integration
* 2-D and 3-D graphics functions for visualizing data
* Tools for building custom graphical user interfaces
* Functions for integrating MATLAB based algorithms with external applications and languages, such as C, C++, FORTRAN, Java, COM, and Microsoft Excel.

# 

# CHAPTER 3



## 3.1. Problem Description

The previous existing system deals with transmission of a message or data without allowing unauthorized access over the internet but with lesser security using the basic approach of Steganography technique. In that approach data was revealed to the receiver only by applying both the keys.Futher the problem with earlier approach was as follows

1. If any one of the key (that is either data hiding key or encryption key) is lost while the transmission of key from sender to receiver then the receiver can’t extract the data.

2. If the mail from the sender does not reach the expected client due to many reasons such as poor availability of network, poor availability of internet or loss of internet, improper mail id entered by the sender.

## 3.2. Proposed Solution

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. In our project we implement the key generation by using SELECTIVE ENCRYPTION. We give additional password to decrypt our image. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the Least Significant Bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image. The algorithm used for the same is Selective Encryption.

## 3.2.1 Selective Encryption

The encryption process requires an encryption algorithm and a key. The process of recovering plaintext from cipher text is called decryption. The accepted view among professional cryptographers (formalized in KIRKHOFF's law) is that the encryption algorithm should be published, whereas the key must be kept secret. Selective encryption scheme generate the key before starting the process of encryption and decryption, rather than storing it. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during encryption and decryption separately. From Fig. 1, it is clear that the receiver should decrypt the information before it can decompress the image. This approach has the main drawback that it is impossible to access the smallest part of information without knowledge of the key. For example, it would impossible to search through a general database of fully encrypted images.

IMAGE

COMPRESSION

KEY1

ENCRYPTION

DECRYPTION

KEY2 2

DECOMPRESSION

IMAGE

. Figure Encryption of image

A way to address this issue is to use a technique called selective encryption; it is depicted in Fig. 2. The image is first compressed (if needed). Afterwards the algorithm only encrypts part of the bit stream with a well-proven ciphering technique; incidentally a message (a watermark) can be added during this process. To guarantee a full compatibility with any decoder, the bit stream should only be altered at places where it does not compromise the compliance to the original format. This principle is sometimes referred to as format compliance.

IMAGE

MESSAGE

COMPRESSION

ENCRYPTION

KEY 1

MESSAGE

IMAGE

DECOMPRESSION

DECRYPTION

KEY 2

Figure Selective encryption mechanism

## 3.3. Design – Steps

The below flowchart shows the design steps

INPUT IMAGE INITIALISATION

IMAGE ENCRYPTION

DATA EMBEDDING

DATA EXTRACTION &

IMAGE RECOVERY

GUI FORMAT

Figure 3 Flowchart Planning

## 3.4. Implementation-Logic Description

In our proposed system, we implement the key generation by using SELECTIVE ENCRYPTION ALGORITHM. In our project there are three phases

The namely Image Encryption, Data embedding and image /data recovery phase an encrypted image. Firstly the image is encrypted using Encryption Key. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data.

At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version.

When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

The image below shows the implementation of the proposed method.

INPUT IMAGE

IMAGE ENCRYPTION

ENCRYPTION KEY

INPUT

ADDITIONAL DATA

HIDE ADDITIONAL DATA

DATA KEY

RECEIVE ENCRYPTED DATA

DATA KEY

TRANSMIT

DECODE

DATA

DECRYPT

IMAGE

ENCRYPTION KEY

Figure 4 Separable reversible data hiding in an encrypted image

## 3.5. Methodology

1. INPUT IMAGE INITIALIZATION:

We initialize the given image (i.e.) get the input image from user by using the keyword ‘uigetfile’. This contains only the pathname and filename. To read the image filename, we used ‘imread’ command. This read image was store in a variable as a matrix. Then we estimate the size of the given image using ‘size’ command. This gives information of size of given image to estimate whether the given text was within the size of input image.

2. IMAGE ENCRYPTION:

Assume the original image with a size of N1XN2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as bi,j,0, bi,j,1,…,bi,j,7 where 1<=i<=N1 and1<=j<=N2, the gray value as, and the number of pixels as N(N=N1XN2). That implies

bi,j,u  = [pi,j /2u]mod 2 , u=0,1,2,…,7

In encryption phase, the exclusive-or results of the original bits and pseudo-random bits are calculated.

3. DATA EMBEDDING:

In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure is as follows. According to a data-hiding key, the data-hider pseudo-randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding.

4. DATA EXTRACTION AND IMAGE RECOVERY:

In this phase, we will consider the three cases that a receiver has only the data-hiding key, only the encryption key, and both the data-hiding and encryption keys, respectively.

With an encrypted image containing embedded data, if the receiver has only the data-hiding key, he may first obtain the values of the parameters and from the LSB of the selected encrypted pixels. Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, although the receiver having the data-hiding key can successfully extract the embedded data, he cannot get any information about the original image content.

5. COMPUTE PSNR VALUE:

We compute the PSNR value for input image and decrypted image. Peak Signal-to-Noise Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined via the mean squared error (*MSE*). Using this PSNR value we can compare our algorithm with other algorithm that our method gives better result than previous method.

# CHA PTER 4

## 4.1. Milestones

There were several milestones set some of few are listed below:

1. Input Image initialization

2. Generation of image encryption key and Image Encryption

3. Data embedding in the input image

4. Generation of data hiding key

5. Recovering data and image

6. Calculation of Peak Signal to Noise Ratio

## 4.2. Achievements

The milestones are successfully achieved. The image is encrypted using encryption key and data is embedded in the image. The data is hidden with the help of data hiding key. Furthermore after the completion of encryption process the data and image is retrieved back by applying the decryption key.

## 4.3. Individual and Team work report

The below table shows the individual work report

Table Individual Report

|  |  |
| --- | --- |
| TEAM MEMBER | WORK ASSIGNED |
| ABHINAV JHA  0812EC141007 | Searched IEEE papers and research paper. Study on cryptography. Worked on non-separable reversible data hiding in an encrypted image. Study on Selective Encryption. MATLAB coding |
| AKSHANSHI JAIN  0812EC141016 | Searched IEEE papers and research paper. Study on cryptography. Worked on study of separable-reversible data hiding in encrypted image. Study on Selective Encryption. Documentation work. MATLAB coding |
| AKSHITA PATHAK  0812EC141019 | Searched IEEE papers and research paper. Study on cryptography. Worked on separable reversible data hiding in an encrypted image.Study on Selective Encryption. Documentation work. MATLAB coding. |
| AMAN THAKUR  0812EC141025 | Searched IEEE papers and research paper. Study on cryptography. Worked on study of non-reversible data hiding in encrypted image.Study on Selective Encryption. MATLAB coding. |



# chapter 5

**RESULT**

This image includes the process of Input Image Initialization, Generation of Encryption key, Data Embedding and Generation of Data hiding key.

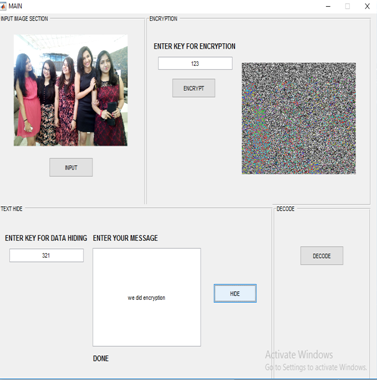


Figure Output at the sender’s side

This image includes the process of Extraction of Image and the Data independently by applying Decryption key. Also calculation of PSNR value is done.

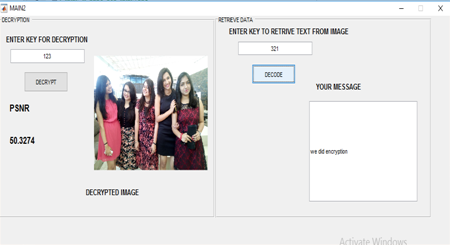
****

Figure Output at the receiver's side

# CHAPTER 6



## 6.1. Conclusion and Future Scope

In this project data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image-recovery phases by using

Selective Encryption method. Here we include another key act as password to decrypt the encrypted image. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

**FUTURE ENHANCEMENT**

In future, we implement this process of image encryption and data hiding in video sequence efficiently.

# References

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[4] S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[5] X. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[8] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, “Lossless generalized- LSB data embedding,” IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

[9] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, “A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification,” Signal Process., vol. 90, pp. 2911–2922, 2010.

[10] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, “Reversible data-embedding scheme using differences between original and predicted pixel values,” IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.