**A New Rule for Cost Reassignment in Adaptive Steganography**

**INTRODUCTION**

Steganography is a technique for covert communication, which aims to hide secret messages into ordinary digital media without drawing suspicion. Designing steganography algorithms for various cover sources is challenging due to the fundamental lack of accurate models. Currently, the most successful approach for designing content adaptive steganography is based on minimizing the distortion between the cover and the corresponding steno object. The distortion is obtained by assigning a cost to each modified cover element (e.g., pixel in the spatial domain image), and the messages are embedded while minimizing the total distortion which is the sum of costs of all modified elements.

**SCOPE OF THE PROJECT**

We propose a cost reassignment scheme. Through extensive experiments on several kinds of steno algorithms, steganalysis features and cover databases; we demonstrate that the CPP rule can improve the security of state-of-the-art steganography algorithms for spatial images.

**LITERATURE SURVEY**

**Title :** A Short Survey on Image Steganography and Steganalysis Techniques

**Author :** Yam Bern Jina Chan, ThemrichonTuithung, Kh. Manglem Singh

**Year :** 2014

**Description :** The paper describes a short survey on different types of steganography techniques for image in spatial and transform domains and steganalysis techniques for the detection of secret message in the image. The strong and weak points of these techniques are mentioned briefly so that researchers who work in steganography and steganalysis gain prior knowledge in designing these techniques and their variants. One can develop a better steganography technique by analyzing the contemporary steganalysis techniques.

**Title :** Defining Cost Functions for Adaptive Steganography at the Micro scale

# Author : Kejiang Chen, Weiming Zhang, Hang Zhou, Nenghai Yu.

**Year :** 2015.

**Description :** In the framework of minimizing embedding distortion steganography, the definition of cost function almost determines the security of the method. Generally speaking, texture areas would be assigned low cost, while smooth areas with high cost. However, the prior methods are still not precise enough to capture image details. In this paper, we present a novel scheme of defining cost function for adaptive steganography at the micro scale. The proposed scheme is designed by using a “microscope” to highlight fine details in an image so that distortion definition can be more refined. Experiments show that by adopting our scheme, the current steganographic methods (WOW, UNIWARD, HILL) will achieve better performances on

resisting the state-of-the-art steganalysis.

**Title :** Gibbs Construction in Steganography

**Author :** Tomáˇs Filler*,* Jessica Fridrich

**Year :** 2013

**Description :** We make a connection between steganography design by minimizing embedding distortion and statistical physics. The unique aspect of this work and one that distinguishes it from prior art is that we allow the distortion function to be arbitrary, which permits us to consider spatially dependent embedding changes. We provide a complete theoretical framework and describe practical tools, such as the thermodynamic integration for computing the rate-distortion bound and the Gibbs sampler for simulating the impact of optimal embedding schemes and constructing practical algorithms. The proposed framework reduces the design of secure steganography in empirical covers to the problem of finding local potentials for the distortion function that correlate with statistical delectability in practice. By working out the proposed methodology in detail for a specific choice of the distortion function, we experimentally validate the approach and discuss various options available to the steganographer in practice.

**Title :** Rich Models for Steganalysis of Digital Images

**Author :** Jessica Fridrich*,*  Jan Kodovský

**Year :** 2016.

**Description :** We describe a novel general strategy for building steganography detectors for digital images. The process starts with assembling a rich model of the noise component as a union of many diverse sub models formed by joint distributions of neighboring samples from quantized image noise residuals obtained using linear and nonlinear high-pass filters. In contrast

to previous approaches, we make the model assembly a part of the training process driven by samples drawn from the corresponding cover- and steno-sources. Ensemble classifiers are used

to assemble the model as well as the final steganalyzer due to their low computational complexity and ability to efficiently work with high-dimensional feature spaces and large training sets. We demonstrate the proposed framework on three steganographic algorithms designed to hide messages in images represented in the spatial domain: HUGO, edge-adaptive algorithm by Luo, and optimally coded ternary 1 embedding. For each algorithm, we apply a simple sub model-selection technique to increase the detection accuracy per model dimensionality and show how the detection saturates with increasing complexity of the rich model. By observing the differences between how different sub models engage in detection, an interesting interplay between the embedding and detection is revealed. Steganalysis built around rich image models combined with ensemble classifiers is a promising direction towards automat zing steganalysis for a wide spectrum of steganographic schemes.

**Title :** Designing steganographic distortion using directional filters

**Author :** Vojtˇech Holus and Jessica Fridrich

**Year :** 2012.

**Description :** This paper presents a new approach to defining additive steganographic distortion in the spatial domain. The change in the output of directional high-pass filters after changing one pixel is weighted and then aggregated using the reciprocal Holders norm to define the individual pixel costs. In contrast to other adaptive embedding schemes, the aggregation rule is designed to force the embedding changes to highly textured or noisy regions and to avoid clean edges. Consequently, the new embedding scheme appears markedly more resistant to steganalysis using rich models. The actual embedding algorithmic realized using syndrome-trellis codes to minimize the expected distortion for a given payload.

**EXISTING SYSTEM**

Most modern secure image steganographic schemes define distortion functions for constraining the embedding changes to those parts of the image that are difficult to model such as textured or noisy regions. We present a two-player zero-sum game between steganographer and attacker related to the security of practical steganography.

**MODULES**

**Patient**

* Authentication
* Register details

**ADMIN**

* Authentication
* Encrypt image
* Get data details
* Get reserve point/data/send
* View sender/receiver details

**RECEIVER**

* Extract original data

**MODULE DESCRIPTION**

**PATIENT**

**Authentication**

**Registration**

If you are the new user going to login into the application then you have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password.

Necessary details

Database

**Login**

The user needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself.

LOGIN

CHECK

Proceed to next stage

Hierarchy

DB

**Register Secret details**

In this module after successful**,** Authentication success then doctor registers the patient details.

Database

Doctor

Give Details about patient

Sharing

**ADMIN**

**Authentication**

The Admin needs to enter exact username and password. If login success means it will take up to upload page else it will remain in the login page itself.

LOGIN

CHECK

Proceed to next stage

Hierarchy

**Encrypt cover medium**

After login success admin can encrypt image for the user data, i.e. for the secret message of the user then he will encrypt the image along with the data.

Admin

Image encryption

(Histogram shift)

Get key

**Embed the data**

After login success admin can get patient data, after that encrypted data embed into image and send to receiver side.

Admin

AES encryption (data)

Data hiding key

Embed data into image

**Reserve Point**

Admin send the reserve point of image to receiver, this is the key for the receiver to get the encrypted details of the patient.

Admin

Login

Send to Receiver

Get reserve point

**View patient/doctor details**

In this module, after successful login of the admin the admin have rights to view all details, i.e. Admin can view the patient /doctor details.

Admin

View patient/doctor detail

Database

**RECEIVER**

**Extract data**

In this module after success authentication of the receiver, he will extract the original data from embedded image that was provided by the admin.

Receiver

Original data

Hierarchy

Extract by data hiding key

**GIVEN INPUT AND EXPECTED OUTPUT**

**ADMIN**

**Authentication**

Input: Provide username and password to get permission for access.

Output: View Sender/Receiver details.

**Embed the data**

Input: Encrypt Image and data.

Output: Embed the both.

**RECEIVER**

**Extract data**

Input: Receive/Get data.

Output: Extract original data.

**SENDER**

**Authentication**

Input: Provide username and password to get permission for access.

Output: Send detail to receiver.

**Register**

Input: Provide patient details.

Output: Encrypted format.

**TECHNIQUE USED OR ALGORITHM USED**

**TBIR-Topic diversity**

We found an interesting phenomenon. Namely, that some steganographic methods have a very similar Security performance while defining distortions in very different ways. Among these methods, there is a distinguishment on the costs assignment for some pixels; in other words, the costs assigned on some pixels are large in one method but small in another. We define these pixels as *“controversial pixels”* Because they are assigned with very different costs in different algorithms. Even with such a discrepancy, some of these algorithms can still provide the same level of security. This phenomenon implies that modifications on such controversial pixels have little effect on features of steganalysis.

**HARDWARE AND SOFTWARE REQUIREMENTS**

**SOFTWARE REQUIREMENTS**

* Operating system : Windows7 SP1,8,8.1
* IDE : Microsoft Visual Studio .Net 2013
* Front End : ASP.NET
* Coding Language : C#
* Backend : SQL Server 2012

**HARDWARE REQUIREMENTS**

* Processor : Pentium Dual Core 2.00GHZ
* Hard disk : 140 GB
* Mouse : Logitech.
* RAM : 4GB(minimum)
* Keyboard : 110 keys enhanced.

**SYSTEM DESIGN**

**USE CASE DIAGRAM**

A use case diagram is a type of behavioral diagram created from a Use-case analysis. The purpose of use case is to present overview of the functionality provided by the system in terms of actors, their goals and any dependencies between those use cases.

View sender/receiver details

Register secret details

Authentication

Encrypt image/data

Receiver

Extract data

Admin

Embed data into image

Extract image

Sender

**CLASS DIAGRAM**

A class diagram in the UML is a type of static structure diagram that describes the structure of a system by showing the system’s classes, their attributes, and the relationships between the classes.

Private visibility hides information from anything outside the class partition. Public visibility allows all other classes to view the marked information.

Protected visibility allows child classes to access information they inherited from a parent class.

Doctor



name



password



address



phone



Authentication()



Register secret detail()



share()

Admin



name



password



authentication()



get sender detail()



encrypt image/data()



embedd data into image()



Send reserve point/data()

Database



Senderdetail



Receiver detail



file()



report()

Receiver



Get embedd data()



Extract original data()

**OBJECT DIAGRAM**

An object diagram in the Unified Modeling Language (UML) is a diagram that shows a complete or partial view of the structure of a modeled system at a specific time.

An Object diagram focuses on some particular set of object instances and attributes, and the links between the instances. A correlated set of object diagrams provides insight into how an arbitrary view of a system is expected to evolve over time.

Username= Admin/ Sender/Recevier

Password=\*\*\*\*\*

View Sender/Receiver details

Register Army details/share

Get data/Encrypt image/data

View sender details

Get Merger Point/send

Login

Admin

Sender

Admin

Admin

Extract original data

**STATE DIAGRAM**

A state diagram is a type of diagram used in computer science and related fields to describe the behavior of systems. State diagrams require that the system described is composed of a finite number of states; sometimes, this is indeed the case, while at other times this is a reasonable abstraction. There are many forms of state diagrams, which differ slightly and have.

Login

Get Sender

details

Register Secret

Detail

Encrypt image/

data

Send Embed data

/reserve point

View Sender/Recevier detail

Share

View secret report

Logout

View Sender/Receiver detail

**ACTIVITY DIAGRAM**

Activity diagram are a loosely defined diagram to show workflows of stepwise activities and actions, with support for choice, iteration and concurrency. UML, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. UML activity diagrams could potentially model the internal logic of a complex operation. In many ways UML activity diagrams are the object-oriented equivalent of flow charts and data flow diagrams (DFDs) from structural development.

Get secret

details

Send Embed data

/reserve point

View receiver detail

Logout

Authenticate

Encrypt image/

data

Register Secret

Detail

Share

View Secret report

View sender/Receiver detail

**SEQUENCE DIAGRAM**

A sequence diagram in UML is a kind of interaction diagram that shows how the processes operate with one another and in what order.

It is a construct of a message sequence chart. Sequence diagrams are sometimes called Event-trace diagrams, event scenarios, and timing diagrams.

The below diagram shows the sequence flow shows how the process occurs in this project.

Receiver

Admin

Database

Authentication

Ask details to sender

Authentication

View secret details

Share

Logout

Embed data into image

Sender

Authentication

View sender/Receiver details

Encrypt image/data

Send data/reserve point

Get data and extract to original data

**COLLABORATION DIAGRAM**

A collaboration diagram show the objects and relationships involved in an interaction, and the sequence of messages exchanged among the objects during the interaction.

The collaboration diagram can be a decomposition of a class, class diagram, or part of a class diagram. It can be the decomposition of a use case, use case diagram, or part of a use case diagram.

The collaboration diagram shows messages being sent between classes and object (instances). A diagram is created for each system operation that relates to the current development cycle (iteration).

Sender

Receiver

Database

8: Check legal user

Admin

2: View Secret details

12: Extract original data

1: Ask suggestion to Sender

4: Get Secret date

6: Authentication

7: View Sender/Receiver details

9: View Sender report

3: register Secret details

10: Encrypted data/image

11: Embed data/send

**COMPONENT DIAGRAM**

Components are wired together by using an *assembly connector* to connect the required interface of one component with the provided interface of another component. This illustrates the service consumer - service provider relationship between the two components.

An assembly connector is a "connector between two components that defines that one component provides the services that another component requires. An assembly connector is a connector that is defined from a required interface or port to a provided interface or port."

When using a component diagram to show the internal structure of a component, the provided and required interfaces of the encompassing component can delegate to the corresponding interfaces of the contained components.

Receiver

Admin

Database

Sender

**DATA FLOW DIAGRAM**

A data flow diagram (DFD) is a graphical representation of the “flow” of data through an information system. It differs from the flowchart as it shows the data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts.

**Level 0:**

Admin

Login

Database

ADMIN /USER

LOGIN

DATABASE

ADMIN /USER

LOGIN

DATABASE

ADMIN /USER

LOGIN

DATABASE

ADMIN /USER

LOGIN

DATABASE

**Level 1:**

Register

Database

**Level 2:**

Sender

Send secret details

**Level 3:**

View sender/ receiver detail

Database

**Level 4:**

Get secret data/ encrypt image/data

Admin

**Level 5:**

Get reserve point

Embed data/reserve point

Send to client

**Level 6:**

Receiver

Get encrypted data

Extract data from image

Data

**All Levels:**

Get data/encrypt image data

Share

View Secret details

Embed data into image

Send data/reserve point

View sender/ receiver detail

Admin

/Receive/Sender

LOGIN

DATABASE

View Secret details

Send secret data

Receiver

Extract data

**E-R DIAGRAM**

In software engineering, an entity-relationship model (ERM) is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database, and its requirements in a top-down fashion. Diagrams created by this process are called entity-relationship diagrams, ER diagrams, or ERDs.

An entity-relationship (ER) diagram is a specialized graphic that illustrates the relationships between entities in a database. ER diagrams often use symbols to represent three different types of information. Boxes are commonly used to represent entities. Diamonds are normally used to represent relationships and ovals are used to represent attributes

Login

Admin

Sender

Receiver

**SYSTEM ARCHITECTURE**

Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks. They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

DATABASE

SENDER

RECEIVER

ADMIN

View Secret details

Register/Send secret details

View Sender/Receiver details

Get image/data

Encryption

3DES encryption (data)

Histogram shift (Encrypted domain-image)

Data hiding key

SEND

Get reserve point

Embedded data

Reserve point

Get embed data/reserve point

Extract data/image

Data hiding key

3DES decryption

**Module Diagram**

**FUTURE ENHANCEMENT**

**Description**

The CPP rule considers a combination of several existing methods instead of remaining fixed on a single method. An essential principle in selecting candidate algorithms for the CPP rule is that basic methods have comparable security performances. In addition, the CPP rule provides a novel tool for designing steganographic schemes. In our future work, applying the CPP rule to other covers such as JPEG image, videos, and text, is an interesting direction.

**ADVANTANGES**

* Thermodynamic integration.
* Rate-distortion bound.

**APPLICATIONS**

* Military operation
* Highly confidential data sharing

**CONCLUSION**

The proposed framework reduces the design of secure steganography in empirical covers to the problem of finding local potentials for the distortion function that correlate with statistical delectability in practice. By working out the proposed methodology in detail for a specific choice of the distortion function, we experimentally validate the approach and discuss various options available to the steganographer in practice.

**REFERENCES OR BIBLIOGRAPHY**

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms and Applications. Cambridge University Press, 2009.

[2] B. Li, J. He, J.w. Huang, and Y. Q. Shi , “A survey on image steganography and steganalysis,” *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142-172, 2011.

[3] T. Penny, T.Filler, and T. Bas, “Using high-dimensional image models to perform highly undetectable steganography,” *Proc. of International Workshop on Information Hiding*, vol. LNCS 6387, pp. 161-177, Jun. 28-30, 2010.

[4] T. Penny, P. Bas, and J. Fridrich, “Steganalysis by subtractive pixel adjacency matrix,” *IEEE Trans. on Inf. Forensics and Security* , vol. 5, no. 2, pp. 215-224, Jun. 2010.

[5] V. Holus and J. Fridrich, “Designing steganographic distortion using directional filters,” *Proc. of IEEE Workshop on Information Forensic and Security*, pp. 234-239, Dec. 2-5, 2012.

[6] J. Fridrich and J. Kodovsk´y, “Rich models for steganalysis of digital images ,” *IEEE Trans. on Inf. Forensics Security*, vol. 7, pp. 868-882, Jun. 2012.

[7] T. Denemark, V. Sleigh, V. Holus, R. Corinne, and J. Fridrich, “Selection-channel-aware rich model for steganalysis of digital images,” *Proc. of 6th IEEE International Workshop on Information Forensics and Security*, Atlanta, GA, USA, Dec. 3-5, 2014.

[8] W. X. Tang, H. D. Li, W. Q. Luo, and J. W. Huang, “Adaptive Steganalysis Based on Embedding Probabilities of Pixels,” *IEEE Trans. on Inf. Forensics Security*, vol. 11(4), pp. 734-745, Apr. 2016.

[9] T. Denemark and J. Fridrich, “Improving Selection-Channel-Aware Steganalysis Features,” *Proc. of IS*&*T, Electronic Imaging, Media Watermarking, Security, and Forensics 2016*, San Francisco, CA, Feb. 14-18, 2016.

[10] V. Haul and J. Fridrich, “Digital image steganography using universal distortion,” *Proc. of ACM Workshop on Information hiding and multimedia security*, pp.59-68, Jun. 17-19, 2013.