Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

Received on: 03-03-2014
Accepted on: 15-03-2015
Published on: 20-03-2015

Rizwan Mehdi, Sachin Bhalake, Shashikant Nagdive, Avinash Kidangumuruppel
Indira College of Engineering, Pune
rizwanmhd46@gmail.com
sachinbhalake@yahoo.com
shashikant.nagdive@gmail.com
avinashsatyan5@gmail.com

QR Code for Mobile users

Conflict of Interest: None Declared

Secured Robust Video Data Hiding

Rizwan Mehdi, Sachin Bhalake, Shashikant Nagdive, Avinash Kidangumuruppel
Indira College of Engineering Pune.

ABSTRACT
Video data hiding is a very important research topic. We propose a new video data hiding method that makes use of correction capability of repeat accumulate codes and superiority of forbidden zone data hiding (FZDH). FZDH is used when no alteration is allowed in data hiding process. The framework will support all kind of videos such as .mp4, .3gp, .avi etc. The proposed scheme is, while hiding the video we provide extra security of encryption and decryption.

Keywords: FZDH, data hiding, encrypt process, decrypt process, superiority

Cite this article as:
Rizwan Mehdi, Sachin Bhalake, Shashikant Nagdive, Avinash Kidangumuruppel, Secured Robust Video Data Hiding. Asian Journal of Engineering and Technology Innovation 03 (06); 2015; 22-25.

INTRODUCTION

Data hiding is the process of embedding information into a host medium. In general, visual media are normally preferred due to their wide presence and the tolerance of human perceptual systems involved. The general structure of data hiding process does not depend on the host media type, but the methods in it also varies depending on the nature of such media. For example, image and video data hiding share many common points, however video data hiding have more complex designs due to the additional temporal dimension in contrast to image data hiding. Therefore, video data hiding is used in active research area.

PROBLEM DOMAIN

The major drawback of host activity based methods is that this activity are collected from each stepping stone which are not trustworthy. Since the attacker or the cracker is assumed to have full control over each stepping stone, it can easily modify, delete or forge user login information. This defeat the ability to correlate based on host activity**.**

LITERATURE SURVEY

ErsinEsen and A. AydinAlatan[1] proposed a new video data hiding method that makes use of erasure correction capability of RA codes and superiority of FZDH. Proposed method utilizes selective embedding technique which is used to determine host signal samples suitable for data hiding. This method also contains a temporal synchronization scheme in order to hold frame drop and insert attacks. The proposed framework is tested by typical broadcast material against MPEG-2, H.264 compression, frame-rate conversion attacks, as well as other well-known video data hiding methods. The decoding error values are reported for typical system parameters. The simulation results indicate that such framework can be successfully utilized in video data hiding applications. In this paper, a new block-based selective embedding type data hiding framework is been proposed that encapsulates FZDH and RA codes in accordance with an additional temporal synchronization mechanism. FZDH is a practical data hiding method, which is shown to be superior to the conventional QIM. An important point to be noted is that, a new video data hiding frame- work that makes use of erasure correction capability of RA codes and superiority of FZDH is proposed. Alteration is avoided by using FZDH and this method is also robust to frame manipulation attacks via frame synchronization markers. But, the disadvantage is that the framework involves a number of thresholds (T0, T1, and T2), which are determined manually. The range of these thresholds can be analyzed by using a training set, then some of the heuristics can be deduced for proper selection of these threshold values.

Vectors XikaiXu, Jing Dong et.al.[3] focus on detecting data hiding in motion vectors of compressed video and proposed a new steganalytic algorithm based on the mutual constraints of motion vectors. The constraints of motion vectors from different frames are analyzed and formulized by three functions, and then statistical features are featured out based on these functions. Moreover, author proposes calibration method to improve the detection accuracy. Experimental results shows that the proposed method can effectively attack typical motion-vector-based video steganography. As compared to other proposals this method is used due to its higher performance. But, this method needs to be tested in attacking more steganography algorithms; it is convinced that the constraints of motion vectors (MVs) are helpful for steganalysis. This new idea might suggest new issues for working in this field. It is expected that the constraints of MVs may play a greater role in the future if author can find a better way to describe and measure the statistical changes of such constraints.

SOFTWARE DESIGN

A. General

An object-oriented methodology or approach was used to develop this project, which consists of function and procedures. It can be stated that software can be developed by building self-contained modules as objects that can be easily replaced, modified and reused. In this environment software is a collection of discrete objects that encapsulate their data as well as the functionality to model real world “objects”. Each object has its own attribute and methods. Objects are grouped into classes. Here each object is responsible for itself.

The main focus of the analysis phase of Software development is on “What needs to be done”. The objects obtained during the analysis can serve as the framework or Design. The class’s attributes, methods and association identified during analysis must be designed for implementation language. New classes must be introduced to store intermediate results during the program execution.

During the Design phase, we have to elevate the model into logical entities, some of which might relate more to the computer domain as people or employees. Here the goal is to design the classes that we need to implement the system and the difference is that, at this level we focus only on the view and access classes, such as how to maintain information or the best way of interact with a user or present information.

B .Design process:

During the design phase the classes which were identified in object-oriented analysis must be revisited with a shift focus to their implementation. New classes or attribute and Methods must be an added for implementation purposes and user interfaces. The object-oriented design process consists of the following activities:

1. The design axioms are normally applied to design classes, their attributes, methods, associations, structure and protocols. Refine and complete the static UML class diagram by adding details to the UML diagram. This step consists of following activities.

- Refine attributes.
- Design methods and protocols by utilizing a UML activity diagram to represent the method's algorithms.
- Refine associations between classes
- Refine class hierarchy and design with inheritance
- Iterate and refine again

2. Design the access layer

- Create mirror classes: For every business classes separate classes are identified and created. For Instance, if there are three business classes, create three access layer classes.
- Identify access layer class relationships.
- Simplify classes and their relationships: The main goal here is to eliminate redundant classes and structures.
  - Redundant classes: Avoid using two classes that perform same operation or activities. Simply select one and eliminate the other.
  - Method classes: Revisit the classes that consist of only one or two methods
  - To see if they can be eliminated or combined with existing classes.

Define the view layer classes

- Design the macro level user interface, by identifying view layer objects.
- Design the micro level user interface, which includes the following activities:

Design the view layer objects by applying the design axioms built a prototype of the view layer interface.

- Test usability and user satisfaction.
- Iterate and refine.

3. Iterate and refine the whole design process. From the class diagram, you get to know which classes you will have to build and which existing classes you can reuse. As you do this, you also begin thinking about the inheritance structure. If you have several classes that seem relates but have specific differences.

Design also must be traceable across requirements, analysis, and design from the Requirements model.

System Architecture

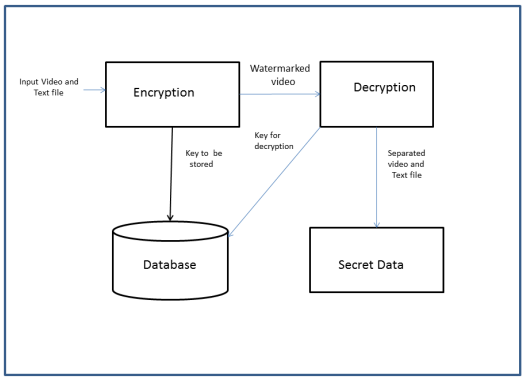

Fig 1: System Architecture

PROPOSED VIDEODATA HIDING FRAMEWORK

A block based adaptive video data hiding method that incorporates FZDH, which is shown to be superior to QIM and competitive with DC-QIM, and erasure handling through RA Codes. We utilize selective embedding to determine which host signal coefficients will be used in data hiding as in. Unlike the method in, we employ block selection (entropy selection scheme) and coefficient selection (selectively embedding in coefficients scheme) together. The de-synchronization is handled in different ways in different selection methods. The de-synchronization due to block selection is handled via RA Codes. The de-synchronization due to coefficient selection is handled by using multi-dimensional form of FZDH in varying dimensions. The frames are processed independently. It is observed that intra and inter frames do not yield significant differences. Therefore, in order to overcome such local bursts of error, we utilize 3-D interleaving similar to, which does not utilize selective

embedding, but uses the whole LL sub band of discrete wavelet transform. Furthermore, we equip the method with frame synchronization markers in order to handle frame drop, insert, or repeat attacks. Hence, it can be stated the original contribution of this paper is to show a complete video data hiding method that is resistant to de-synchronization due to selective embedding and robust to temporal attacks, while making use of the superiority of FZDH

REFERENCES

1. A SECURE COVERT COMMUNICATION MODEL BASED ON VIDEO STEGANOGRAPHY Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb The Military Technical College, Cairo, Egypt 11331
2. Complete Video Quality-Preserving Data HidingKokSheik Wong, Student Member, IEEE, Kiyoshi Tanaka, Member, IEEE, Koichi Takagi, and Yasuyuki Nakajima, Member, IEEE
3. A Novel Video Steganography based on Non-uniform Rectangular Partition ShengDun Hu, KinTak U Faculty of Information Technology Macau University of Science and Technology Macau, China hsdlya@hotmail.com, ktu@must.edu.mo
4. Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding ErsinEsen and A. AydinAlatan, Member, IEEE
5. Steganography over Video File using Random Byte Hiding and LSB Technique Ashish T. Bhole1, Rachna Patel2 1,2Department of Computer Engineering, SSBT's COE & T, Bambhori, Jalgaon, India ashishbhole@hotmail.com1, rachna.patel@utu.ac.in2
6. VIDEO STEGANALYSIS BASED ON THE CONSTRAINTS OF MOTION VECTORS XikaiXu, Jing Dong, Wei Wang and Tieniu Tan Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences E-mail: xikaixu@gmail.com, { jdong, wwang, tnt }@nlpr.ia.ac.cn
7. Steganography in Long Term Evolution Systems IwonaGrabska, Krzysztof Szczypiorski Institute of Telecommunications Warsaw University of Technology Warsaw, Poland e-mail: {i.grabska, ksz}@tele.pw.edu.pl
8. SECURED ROBUST VIDEO DATA HIDING USING SYMMETRIC ENCRYPTION ALGORITHMS 1K.Mohan, 2S.E.Neelakandan 1Department of Computer Science & Engineering 2Department of Information Technology 1, 2Thirumalai Engineering College, Kanchipuram
9. M. Schlauweg, D. Profrock, and E. Muller, "Correction of Insertions and Deletions in Selective Watermarking," in IEEE International Conference on Signal Image Technology and Internet Based Systems, SITIS '08, 2008, pp.277—284.
10. E. Esen, Z. Doğan, T. K. Ates, and A. A. Alatan, "Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding,"in IEEE 17th Signal Processing and Communications Applications Conference SIU, 2009.
11. E. Esen and A. A. Alatan, "Forbidden zone data hiding," in IEEE International Conference on Image Processing, 2006, pp. 1393— 1396.