A Secure Data Hiding Using Visual Cryptography

1) Pooja Raosaheb Gangurde,2) Ankita Sanjay Ghandat,3) Sakshi Bhausaheb Sanap, 4)Priyanka Ishwar Patil

Prof. Ghawande Ranjit(Project Guide)

B.E Student, Department Of Computer Engineering, Matoshri College Of EngineeringAnd Research Center, Nashik, Maharashtra, India Savitribai Phule Pune University OfPune.

Abstract— : **Visual cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In this paper, we intend to study the different application areas of Visual Cryptography. Visual Cryptography is a wide area of research used in data hiding, securing images, color imaging, multimedia and other such fields. Visual Cryptography comes in the field of data hiding used in cybercrime, file formats etc. This paper focuses on the application areas of visual cryptography from four different research papers/journals which talk about the most important application areas of visual cryptography.**

Keywords: visual cryptography, encrypted, data hiding, multimedia, color imaging, cybercrime

I. NTRODUCTION

Visual Cryptography is a cryptographic technique which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. In today's computer generation, data security, hiding and all such activities have become probably the most important aspect for most organizations. These organizations spend millions of their currency to just secure their data. This urgency has risen due to increase in cyber theft/ crime. The technology has grown so much that criminals have found multiple ways to perform cybercrime to which the concerned authorities have either less or not sufficient answer to counter. Hence, the method of Cryptography provides the above answers. One of the most majorparts of cryptography is Visual cryptography. It has many usage & application areas, mostly using its internal technique called encryption.

Some of those application areas are talked about in this research paper.Visual cryptography is used specifically in the areas of Biometric security, Watermarking, Remote electronic voting, Bank customer

identification etc. This research paper contains 4 sections.Section 2 talks about the related work and applications in the field of Visual Cryptography. Section 3 gives the Conclusion of the paper followed by References.

II. SYSTEMDEVELOPMENT

Securing Images through Recursive Visual Cryptography Security is probably the most challenging and needed property in today's technological era. Many organizations have spent tremendous amount of money just to acquire this property for all their related projects. Without security, the data of any organization or a single unit is under threat of getting misplaced or completely taken out from existence. Such is the case with image authentication. Its security analysis is performed through a special method known as Visual Cryptography Scheme.

A. Architecture And Design

- **Real-Time Data Communications**

The major effect of using encryption on real-time data communications is on wiretaps. Wiretap provides valuable information about the criminal's intentions, plans and any such rogue activities. Hackers use encryption on real-time data communications to prevent their communication channels to be intercepted by the law enforcement authorities. Internet Relay Chat(IRC) is that channel which enable the hackers to compromise other governmentmachines.

- **ElectronicMail**

The criminals use many different ways to encrypt their data in emails. The most used technique is Pretty Good Privacy(PGP) which provides a key to perform data encryption.[9] This encryption technique is readily available in the Internet for free so, downloading is very easy. Electronic mail is very hard to trace.

- **StoredData**

This is the most commonly used technique by criminals to encrypt their stolen/ confidential data from the law enforcement. Cryptographic Technologies.

Passwords

Hackers/ criminals keeps their PC's password protec ted to keep out intruders. This is an easy and most effectivewayofsecuringone'sidentityfromtherestof

the world. Passwords are used much more often by hackers rather than encryption related techniques.

Compressing Digital

Files Digital compression compresses digital file's size preventing the loss of important details of the file.

Criminals use compression for two benefits: -

a) A decompressed file makes it hard for the law enforcement authorities to seize crucialfiles.

b) Prior to encryption, it can make cracking of system difficult toconduct.

Cyber Crime through Encryption Techniques Cybercrime is rapidly gaining momentum in the technology world. It's attracting many such individuals who either have been involved in thefts of any kind in their past or the ones who have a nag for engaging in criminal activities. Criminals use many different means to hide evidence on computers from law enforcement mainly through encryption and other such methods like steganography, digital compression, passwords etc. These techniques are making the law enforcement's tasks more difficult day-by-day of there is a need to understand how these criminals work and to subsequently find a solution for the same. In the authors have explained the above techniques in detail and how these affect the law enforcement efforts tocounter.

Steganography

Steganography is the method of hiding secret data into another data so that it is even more secured. Criminals use it to trick the concerned authorities into seeing non- existence of files in a hard-disk of computer. A cracker who does not possess the knowledge of the files can be easily mislead and forced to act in a way which can further make their target even more difficult to achieve. The authors have stressed a lot on the ways criminals/ hackers use encryption techniques to steal & extract confidential Government and other important organization's data but not so much on the ways to counter such actions. There is a need to talk about both sides of the argument in such cases. The encryption techniques used by criminals can be countered in a similar manner by the law enforcement authorities usingdecryption (also part of encryption). Some of those techniques are talked about in the above research papers.

A. Hiding Secret Information in Digital Images

We are able to see many different ways in which images are secured from interference of hackers and other such outside intruders. The concept of digital watermarking is used to allow the authorization of owner and prevent outside intrusion, random grids used to hide secret images and use of joint encryption techniques to provide the sameproperty.

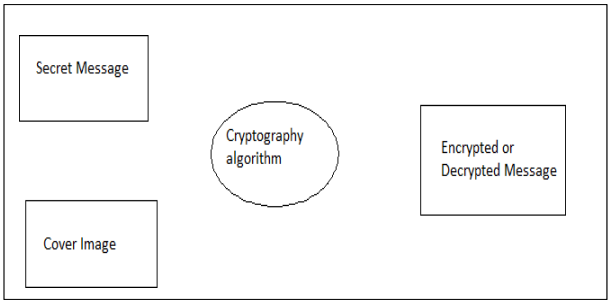
Securing Images through Recursive Visual Cryptography Security is probably the most challenging and needed property in today's technological era. Many organizations have spent tremendous amount of money just to acquire this property for all their related projects. Without security, the data of any organization or a single unit is under threat of getting misplaced or completely taken out from existence. Such is the case with imageauthentication.

Its security analysis is performed through a special method known as Visual Cryptography Scheme (VCS).

Cryptography have found usage in many applications. For example, transmission of attack plans by military teams to hide information about their strategies. Many other applications of data hiding techniques other than its original objective, have gained importance, which include authentication and identification, watermarking and transmitting passwords etc.

Data protection ensures that the Web service re- quest and response have not been tampered with en route. It requires securing both data integrity and privacy. It's worth mentioning that data protection does not guarantee the message sender's identity.which can range from invoking the Web service to executing a certain part of its functionality.

That is, while transmitting the image the sender will encrypt the image using our application here sender gets the two or more transparencies of the same image. Our application provides an option to the end user of encryption



Visual cryptography is one of the technique used to encrypt the images by dividing the original image into transparencies. The transparencies can be sent to the intended person, and at the other end the transparencies received person can decrypt the transparencies using our tool, thus gets the original image. Our proposed Visual cryptography provides the demonstration to the users to show how encryption and decryption can be done to the images. In this technology, the end user identifies an image, which is not the correct image. That is, while transmitting the image the sender will encrypt the image using our application here sender gets the two or more transparencies of the same image. Our application provides an option to the end user of encryption. The end user can divide the original image into number of different images. Using our application we can send encrypted images that are in the format of GIF AndPNG.

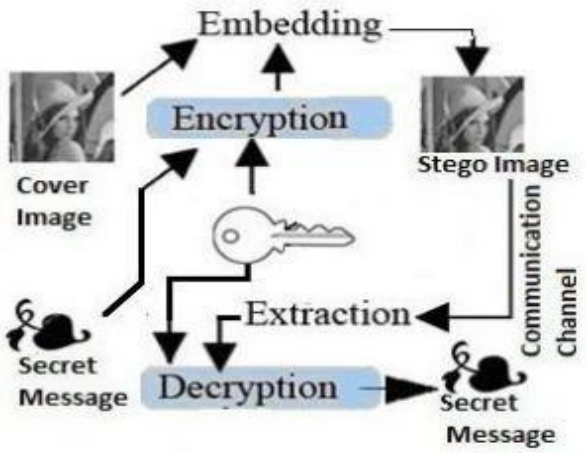


Fig1: Architecture Diagram

This process involves converting a secret image into a text document, then encrypting the generated text into a ciphertext using a image (password) based encryption algorithm, and finally embedding the ciphertext on to a cover image.

A Visual cryptography model facilitates hiding or embedding of sender's secret message in a file (carrier) that does not give out a clue about the existence of secret message in it when viewed.

Is taken as a carrier that can act as cover for the sender's message, that is, a message here is hidden in a carrier and that carrier transmitted. In today, world ,the communication is the basic necessity every rowing area. Everyone wants the secrecy and safety of their communication data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information offshore window power aredifferent

Advantages:

Number of bites have been replace ac With the use of visual cryptography Corporation government and law enforcement agencies can communicate secretly.

This method featured security, capacity, and robustness, the three needed aspects of visual cryptography that makes it useful in hidden exchange of information through text documents and establishing secret communication

Difficult to detect. Only receiver can detect.

This system is security that it provide security to your message without knowing to third party.cording to user or sender, there for third party cannot guess password.

Response Time :1.0 second is about the limit for the user's ow of thought to stay uninterrupted, even though the user will notice the delay. Normally, no special feedback is necessary during delays of more than 0.1 but lessthan 1.0 second,but the user does lose the feeling of operating directly on the data. 10 seconds is about the limit for keeping the user's attention focused on the dialogue. For longer delays, users will want to perform other tasks while waiting for the computer to finish, so they should be given feedback indicating when the computer expects to be done. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what toexpect.

Scalability: The scalability required is of- ten driven by the lifespan and the maturity of the system. For example, a new (and hence immature) system could suffer an unexpected growth in popularity and suffer from a significant increase in workload as it becomes popular with new users. More mature systems which represent improvements on older systems are likely to have more accurately defined workloads and thusbelesslikelytosufferinthisrespect.

Platform: A platform is defined as the underlying hardware and soft- ware (operating system and software utilities) which will house the system. It is not always the case that the designer will be given a ”greenfield” choice of what platform on which to house the system. In some cases the customer may dictate this choice or there may be internalreasons (product strategy perhaps) that will constrain the designer’s freedom. It may also be the case that the system will require various generic products to be used in which case the performance of these must also be sp ecified. I f there is extensive damage to the wide portion of database due to catastrophic failure, like disk crash, the recovery method will restores the past copy of thedatabase.

Software Design Specification:

Introduction

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in specific a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless. Recovery of the image can be done by superimposing specified number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decryptedimage

Purpose

Our project is developed for hiding information in any image file to ensure the safety of exchange the data between different parties and provide better security during messagetransmission.

External InterfaceRequirements

UserInterfaces:

Initially user must have web application to find the nearest changing station and second is charging station should be connected to internet for real-time monitoring.

Hardware Interfaces:

We are using Micro controller which works as a central controller in our system.
Processor: Intel or AMD processor computer

RAM: 256 MB or more.

Hard Disk Space: 8 GB or more

Software Interfaces:

We are using open-source IDE for development purpose.

Operating System: Windows 7,8 and Above

Technologies: JAVA 1.8 , Swing

Tools: Eclipse

Communications Interfaces:

The communication between the different parts of the system is important since they depend on each other. We usually use middle ware for communication between the Java with database.

Other Requirement:

1. DatabaseRequirement

Platform:
Back end MySQLServer.

2. Hardware Requirement

Computer System: RAM 2GB
Hard Disk:80GB
Processor: i3 and above.

UML Diagrams:

Unified Modeling Language (UML) is a general purpose modelling language. The main aim of UML is to define a standard way to visualize the way a system has been designed. It is quite similar to blueprints used in other fields of engineering.

Unified Modeling Language (UML) is a general purpose modelling language. The main aim of UML is to define a standard way to visualize the way a system has been designed. It is quite similar to blueprints used in other fields of engineering.

Use case Diagram

Use Case Diagrams are used to depict the functionality of a system or a part of a system.

They are widely used to illustrate the functional requirements of the system and its interaction with external agents(actors). A use case is basically a diagram representing different scenarios where the system can be used. A use case diagram gives us a high level view of what the system or a part of the system does without going into implementation details.

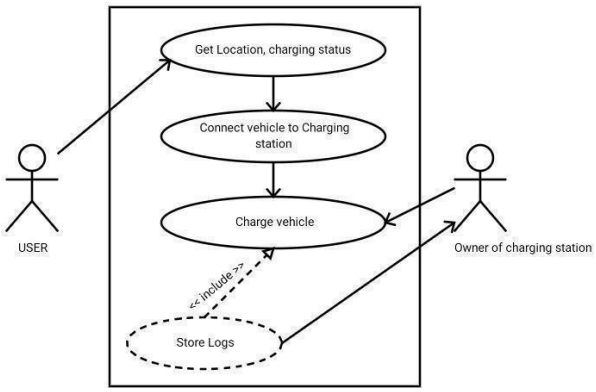


Fig17:Use Case Diagram

Componant Diagram:

We use componant Diagrams to illustrate the flow of control in a system. We can also use an activity diagram to refer to the steps involved in the execution of a use case. We model sequential and concurrent activities using diagrams. So, we basically depict workflows visually using an componant diagram. an componant diagram focuses on condition of flow and the sequence in which it happens. We describe or depict what causes a particular event using an componant diagram.

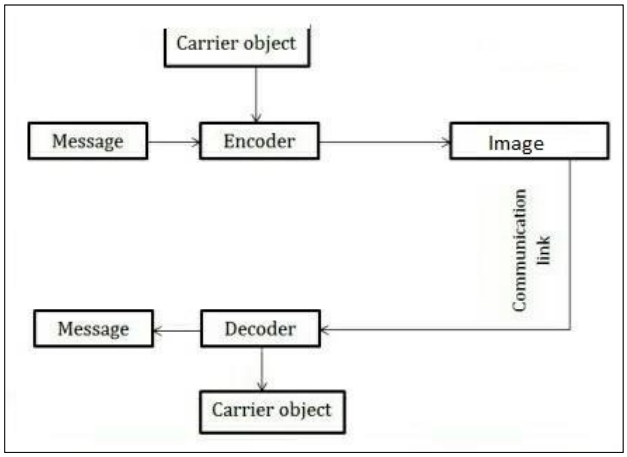


Fig.Componant Diagram

Data Flow Diagram

A Data flow diagram simply depicts interaction between objects in a sequential order i.e. the order in which these interactions take place. We can also use the terms event diagrams or event scenarios to refer to a sequence diagram. Sequence diagrams describe how and in what order the objects in a system function. These diagrams are widely used by businessmen and software developers to document and understand requirements for new and existing systems.

Reliability of a software system is defined as the probability thatthis system fulfills a function (determined by the specifications) for a specified number of input trials under specified input conditionsin a specified time interval (assuming that hardware and input are free oferrors)

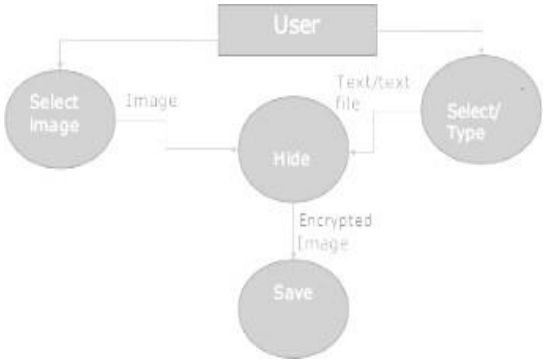


Fig. Data Flow Diagram

Class Diagram:

The most widely use UML diagram is the class diagram. It is he building block of all object oriented software systems.We use class diagrams to depict the static structure of a system by showing system's classes, their methods and attributes. Class diagrams also help us identify relationship between different classes or objects.

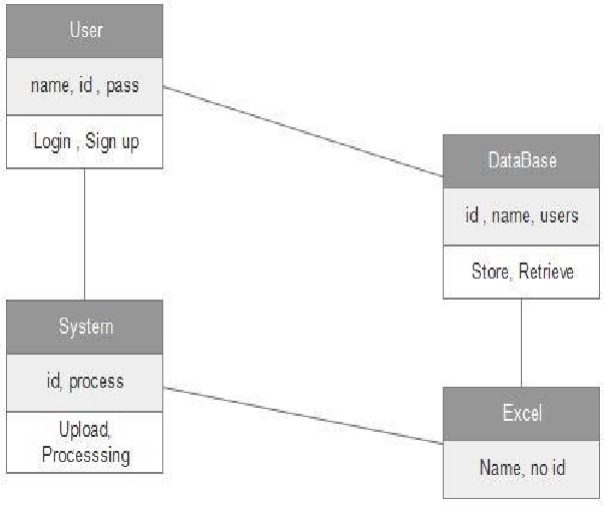


Fig :Class Diagram

To provide a secure form feeling platform for user.Avoid the drawbacks of existing system and provide the proposed system user f r iendly. shouldbeacentralized management system, which allow user to view information.

III. Conclusion

I have learned that while implementing Image cryptography is important, thinking of how to detect and attack it and the methods to do so are far more complex than actually doing the cryptography itself. There is a lot of research that is beginning to discover new ways to detect cryptography, most of which involves some variation of statistical analysis. It is interesting to see what other methods will be developed and how accurate they will be at detecting cryptography.

Appendix

Appendixes, if needed, appear before the acknowledgment.

Acknowledgment

It gives us great pleasure in presenting the preliminary project report on visual cryptography We would like to take this opportunity to thank my internal guide **Mr.Ranjit M. Gawande** for giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.We are also grateful to **Dr.V. H. Patil**, Head of Computer Engineering Department, Matoshri College Of Engineering and Research Centre for her indispensable support, suggestions.In the end our special thanks to **Technical Staff** for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for OurProject.

References

- https://www.scribd.com/document/21741503/visualcryptography.
- Desiha, M.; Kaliappan, V.K., " halftoning technique in embedded extended visual cryptography strategyfor effective processing", vol.5, 8-10 Jan.2015.
- www.ims.nus.edu.sg/program/imgscifiles/memon/sing_stego.pdf
- Som S., Mitra D., Halder J., (2008) "Session KeyBased Manipulated Iteration EncryptionTechnique.
- Ramya, J.; Parvathavarthini, B., "An extensive review on visual cryptography schemes," in Control, Instrumentation, Communication and ComputationalTechnologies (ICCICCT),2014 International Conference on, vol., no., pp.223-228, 10-11 July 2014.