

ELECTRONIC MEDICAL REPORT SHARING USING VISUAL CRYPTOGRAPHY

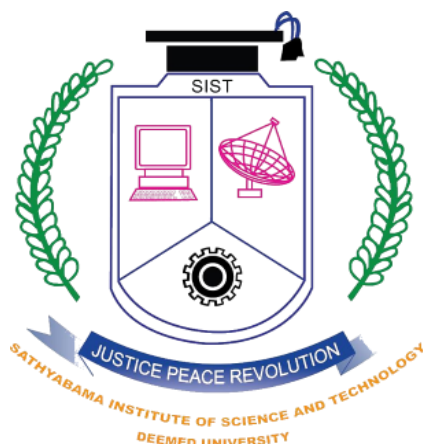
Submitted in partial fulfilment of the required for the award of

Bachelor of Computer Science

by

KABILAN.A

(REGISTER NO 40290040)



DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF SCIENCE AND HUMANITIES

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAR NAGAR, RAJIV GANDHI SALAI, CHENNAI 600 119

MAY 2023



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC I Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **KABILAN.A (40290040)** who carried out the project entitled **“ELECTRONIC MEDICAL REPORT SHARING USING VISUAL CRYPTOGRAPHY”** under our supervision from JANUARY 2023 to MAY 2023.

Internal Guide

Ms. AISHWARYA , MCA., Assistant Professor

DEAN AND HEAD OF THE DEPARTMENT

Dr. REKHA CHAKRAVARTHI M.E., Ph.D.

Submitted for Viva voce examination held on 8.05.2023

Internal Examiner

External Examiner

DECLARATION

I am, **KABILAN.A (40290040)** here by declare that the Project Report entitled **“ELECTRONIC MEDICAL REPORT SHARING USING VISUAL CRYPTOGRAPHY”** done by us under the guidance of **MS.AISHWARYA**, Assistant Professor, Department of Computer Science at **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY**, Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai-600 119 is submitted in partial fulfillment of the requirements for the award of Master of Science degree in Computer Science.

DATE: 08/05/2023

PLACE: CHENNAI



KABILAN.A

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to board of the management of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. REKHA CHAKRAVARTHI M.E., Ph.D. Dean of Arts and Science** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep since of gratitude to my project guide **MS.AISHWARYA.B**, Assistant Professor, Department of Computer Science for their valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff member of the Department of Computer Science who were helpful in many ways for the completion of the project.

KABILAN.A

ABSTRACT

Visual Cryptography Scheme (VCS) is an encryption method used to encode secret written materials. The idea is to convert the written material into a binary image and encode this image into n shadow images. It is also called as shares of images. The decoding only requires selecting some subset of these n shadow images, making transparencies of them and stacking them on top of each other. Main advantage of this scheme is mathematical computation complexity is reduced to visual cryptographic techniques. Each participant holds a transparency. Most of the previous research work on VC's focuses on two parameters: large pixel expansion and contrast. Further, the number of sub pixels (m) for encoding each secret pixel, referred to as the pixel expansion, is the smaller the enhanced to reduce the share size. The pixel expansion and relative contrast are the most critical measurements to evaluate the effectiveness of a VCS. This includes random cipher code generation, training gray relational analysis (GRA)-based encryptor and decryptor, and decrypted image evaluation. We develop a novel and efficient construction for VC using GRA in this project. The first and second GRA models are used to train the cipher codes to achieve an encryptor and a decryptor, respectively. The proposed Visual Cryptograms of Random Grids aims at the minimization of the pixel expansion and maximal contrasts for individual a VC. The Experimental results demonstrate the feasibility, applicability, and flexibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results.

TABLE OF CONTENTS		
CHAPTER	TITLE	PAGE NO
	ABSTRACT	1
	LIST OF FIGURES	viii
1	INTRODUCTION	4
	1.1 ELECTRONIC MEDICAL REPORT SHARING USING VISUAL CRYPTOGRAPHY	
	1.2 SYSTEM OVERVIEW	4
	1.3 SCOPE OF THE PROJECT	5
2	LITERATURE SURVEY	5
3	SYSTEM ANALYSIS	10
	3.1 EXISTING SYSTEM	10
	3.1.1 DISADVANTAGES OF EXISTING SYSTEM	10
	3.2 PROPOSED SYSTEM	11
	3.2.1 ADVANTAGES OF PROPOSED SYSTEM	12
	3.3 REQUIREMENT SPECIFICATION	
	3.3.1 HARDWARE REQUIREMENTS	12
	3.3.2 SOFTWARE REQUIREMENTS	13

4	SYSTEM DESIGN	
	4.1 SYSTEM ARCHITECTURE	14
	4.2 SEQUENCE DIAGRAM	15
	4.3 USE CASE DIAGRAM	16
	4.4 STATE DIAGRAM	18
	4.5 COLLABORATION DIAGRAM	19
	4.6 CLASS DIAGRAM	20
5	MODULE DESCRIPTION	
	5.1 MODULES	21
6	CONCLUSION AND FUTURE ENHANCEMENT	
	6.1 CONCLUSION	24
	6.2 FUTURE ENHANCEMENT	24
	APPENDIX 1	25
	APPENDIX 2	34
	REFERENCES	38

	LIST OF FIGURES	
FIGURE NO	TITLE	PAGE NO
4.1	ARCHITECTURE OF PROPOSED SYSTEM	19
4.2	SEQUENCE DIAGRAM	21
4.3	USE CASE DIAGRAM	22
4.4	STATE DIAGRAM	23
4.5	COMPONENT DIAGRAM	24
4.6	DEPLOYMENT DIAGRAM	25
4.7	COLLABORATION DIAGRAM	26
4.8	CLASS DIAGRAM	27

CHAPTER 1

INTRODUCTION

Visual Cryptography Scheme (VCS) is an encryption method used to encode secret written materials. The idea is to convert the written material into a binary image and encode this image into n shadow images. It is also called as shares of images. The decoding only requires selecting some subset of these n shadow images, making transparencies of them and stacking them on top of each other. Main advantage of this scheme is mathematical computation complexity is reduced to visual cryptographic techniques. Each participant holds a transparency. Most of the previous research work on VC's focuses on two parameters: large pixel expansion and contrast. Further, the number of sub pixels (m) for encoding each secret pixel, referred to as the pixel expansion, is the smaller the enhanced to reduce the share size. The pixel expansion and relative contrast are the most critical measurements to evaluate the effectiveness of a VCS. In this paper, we studied the in VC in addition to Multiple-Secret Visual Cryptographic Schemes (MSVCS) can achieve the minimum pixel expansion and the maximal contrasts.

We develop a novel and efficient construction for VC using MSVCS in this paper. The proposed Visual Cryptograms of Random Grids aims at the minimization of the pixel expansion and maximal contrasts for individual a VC. The Experimental results demonstrate the feasibility, applicability, and flexibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results.

1.3 SCOPE OF THE PROJECT

This project concentrates on the task to provide security features for database system in terms of visual cryptography schemes. In proposed system, to prevent the accessing of data in database, the security is enhanced in three phases using visual cryptography. In this proposed work, to prevent the accessing of data in database the administrator enhances the security using visual cryptography. We use a generic method that converts a VCS to another MSVC's that has the property of cheating prevention.

We show two methods to generate the covering shares, and proved the optimality on the black ratio of the threshold covering subsets. We also proposed a method to improve the visual quality of the share images.

CHAPTER 2

LITERATURE SURVEY

[1]. G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” *Theoretical Computer Sci.*, vol. 250, pp. 143–161, 2001.

An extended visual cryptography scheme (EVCS), for an access structure on a set of n participants, is a technique to encode n images in such a way that when we stack the transparencies associated to participants in any set they got the secret message with no trace of the original images, but any has no information on the shared image. Moreover, after the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency.

[2]. G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Visual cryptography for general access structures,” *Inf. Computat.*, vol. 129, pp. 86–106, 1996.

A visual cryptography scheme for a set of n participants is a method of encoding a secret images I into n shadow images called shares, where each participant in receives one share. Certain qualified subsets of participants can “visually” recover the secret image, but other, forbidden, sets of participants have no information (in an information theoretic sense) on SI . A “visual” recovery for a set $X \subseteq$ consists of xeroxing the shares given to the participants in X onto transparencies, and then stacking them. The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation. In this paper they propose two techniques for constructing visual cryptography schemes for general access structures. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the shares distributed to the participants in the scheme.

[3]. G. Ateniese, C. Blundo, A. De. Santis, and D. R. Stinson, “Constructions and bounds for visual cryptography,” *Lecture Notes Computer Sci.*, vol. 1099, pp. 416–428, 1996.

A visual cryptography scheme for a set P of n participants is a method to encode a secret image SI into n images in such a way that any participant in P receives one image and only qualified subsets of participants can “visually” recover the secret image, but non-qualified sets of participants have no information, in an information theoretical sense, on SI . A “visual” recover for a set $X \subseteq P$ consists of stacking together the images associated to participants in X . The participants in a qualified set X will be able to see the secret image without any knowledge of cryptography and without performing any cryptographic computation.

In this paper they propose two techniques to construct visual cryptography schemes for any access structure. We analyze the structure of visual cryptography schemes and we prove bounds on the size of the image distributed to the participants in the scheme. They provide a novel technique to realize k out of n visual cryptography schemes. Finally, they consider graph-based access structures, that is access structures in which any qualified set of participants contains at least an edge of a given graph whose vertices represent the participants of the scheme. Our constructions for 2 out of n visual cryptography schemes are the best possible with respect to pixel expansion and relative difference.

[4]. C. Blundo, S. Cimato, and A. De Santis, “Visual cryptography schemes with optimal pixel expansion,” *Theoretical Computer Sci.*, vol. 369, pp. 169–182, 2006.

A visual cryptography scheme encodes a black and white secret image into n shadow images called shares which are distributed to the n participants. Such shares are such that only qualified subsets of participants can “visually” recover the secret image.

Usually, the reconstructed image will be darker than the background of the image itself. In this paper we consider visual cryptography schemes satisfying the model introduced by Tzeng and Hu [A new approach for visual cryptography, *Designs, Codes and Cryptography* 27 (3) (2002) 207–227]. In such a model, the recovered secret image can be darker or lighter than the background. We prove a lower bound on the pixel expansion of the scheme and, for $(2,n)$ -threshold visual cryptography schemes, we provide schemes achieving the bound. Our schemes improve on the ones proposed by Tzeng and Hu.

[5]. S. Climato, R. D. Prisco, and A. De. Santis, “Optimal colored threshold visual cryptography schemes,” *Designs, Codes and Cryptography*, vol. 35, pp. 311–335, 2005.

Visual cryptography schemes allow the encoding of a secret image into n shares which are distributed to the participants. The shares are such that only qualified subsets of participants can “visually” recover the secret image. Usually the secret image consists of black and white pixels. In colored threshold visual cryptography schemes the secret image is composed of pixels taken from a given set of c colors. The pixel expansion and the contrast of a scheme are two measures of the goodness of the scheme.

In this paper, they studied c -color (k,n) -threshold visual cryptography schemes and provide a characterization of contrast-optimal schemes. More specifically we prove that there exists a contrast-optimal scheme that is a member of a special set of schemes, which we call *canonical schemes*, and that satisfy strong symmetry properties.

Then they use canonical schemes to provide a constructive proof of optimality, with respect to the pixel expansion, of c -color (n,n) -threshold visual cryptography schemes.

Finally, they provide constructions of c -color $(2,n)$ -threshold schemes whose pixel expansion improves on previously proposed schemes.

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

Image degradation will occur due to pixel expansion and Contrast level. Hacker may easily verify the irregular color appearance in the stego image. The existing visual cryptography schemes that are used for data hiding have a security hole in the encrypted Share file. If the share images are hacked, the hacker can tamper the data that is hidden and hence can disturb the entire technique. In the existing, there is no optimized secured way to access the secret hidden data and the data that are stored in databases

3.1.1 Disadvantages of the Existing System

- The existing system does not provide a friendly environment to encrypt or decrypt the data (images).
- The existing system supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.
- Data confidentiality, data integrity, and data availability for information communication is not Ensured.

3.2 PROPOSED SYSTEM

In recent years, some studies have been developed for medical signal and image cryptographic applications using chaotic maps, including sine/cosine-power maps, circle maps, tent maps, and logistic maps.

- The most important result is the improvement of the visual quality of both the share images and the stack image to their theoretical maximum.
- Experimental results demonstrate the feasibility, applicability, and flexibility of our construction. The pixel expansions and contrasts derived from our scheme are also better than the previous results.
- First, an image is split into “n” encrypted shares using algorithm by the fact that a pixel can be split into sub pixels.
- Second, in order to avoid hacking of shared image, we employ password protection for each share using Embedded algorithm and simple Arithmetic Encoding compression technique which compresses the pass code.
- Third, we perform rearranging of pixels of shared image by overlaying process to obtain the access to the protected data's.
- Image encryption techniques include the permutation method or rearranging numerical or pixel positions and substitution method or changing numerical or pixel values which have secret keys in the symmetric cryptography protocol against active hacker or passive hacker attacks.
- This project concentrates on the task to provide security features for database system in terms of visual cryptography schemes. In proposed system, to prevent the accessing of data in database, the security is enhanced in three phases using visual cryptography.
- First, an image is split into n encrypted shares using algorithm by the fact that a pixel can be split into sub pixels. Second, in order to avoid hacking of shared image, we employ password protection for each share using Multiple Secret Visual cryptography algorithm and simple Arithmetic Encoding compression technique which compresses the pass code. Third, we perform rearranging of pixels of shared image by overlaying process to obtain the access to the protected database.

3.2.1 Advantages of the Proposed System

- It is used to enhance the chaotic complexity .
- It also expand large chaotic ranges for increasing the key space for selecting pseudorandom keys.
- It also generate unpredictable cipher codes.

3.3 REQUIREMENTS SPECIFICATION

Hardware Requirements

- Processor : intel core i5
- RAM : 4GB
- Keyboard : 104 Keys
- Hard disk : 500GB
- Network : 1mbps

3.3.2 Software Requirements

- Program language : Java, Java Swing
- Operating System : Windows 10
- Platform : JDK 1.5 or 1.6

CHAPTER 4

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

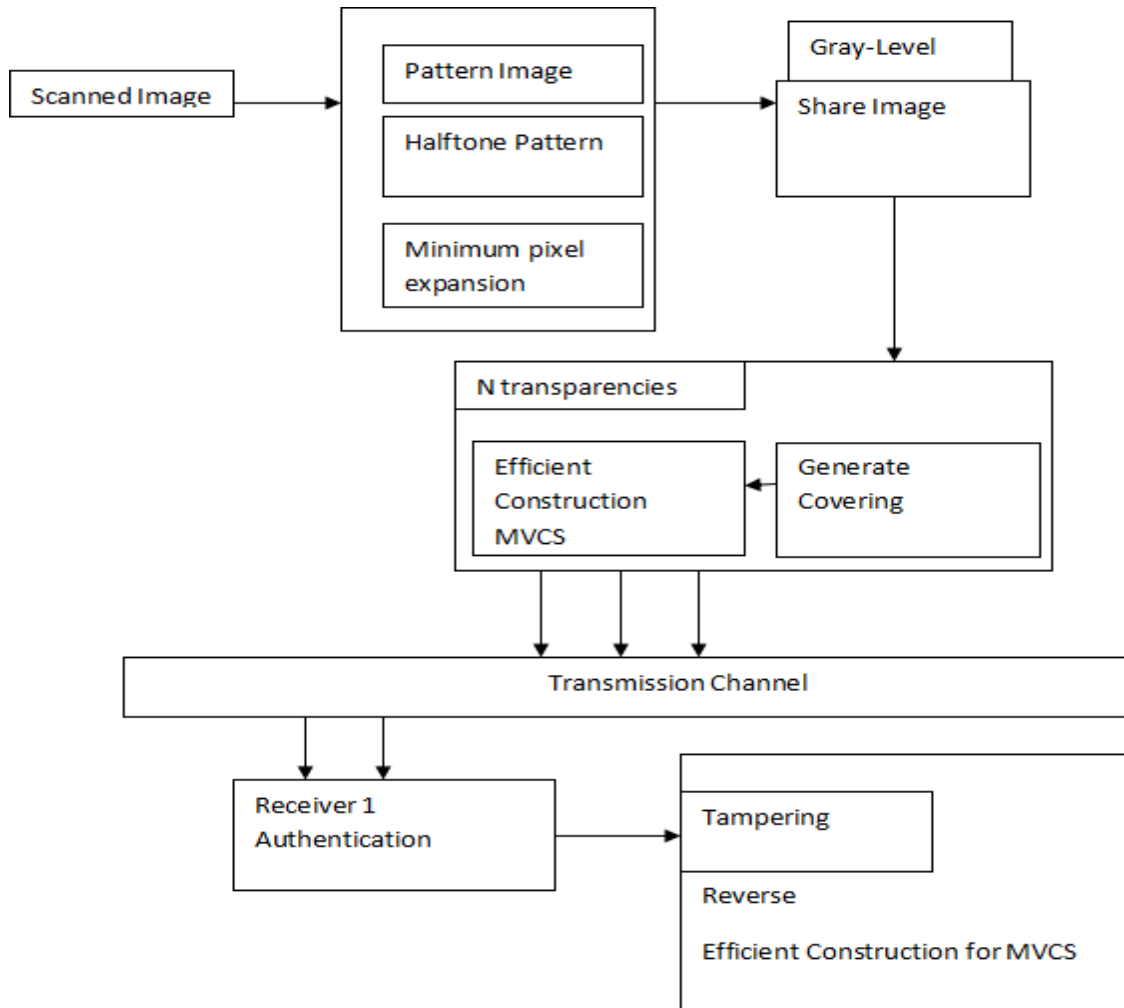


Figure 4.1 Architecture of proposed system

User provides a secret image and outputs of Original shares image which relevant for secret. We can satisfy with the two conditions: 1. any qualified subset of shares can recover the secret image; any forbidden subset of shares cannot obtain. 2. any information of the secret image other than the size of the secret image.

We can obtain the original image with only k shares out of n shares, then all the ' n ' image shares are necessarily overlaid. When all the image shares that are overlaid are authenticated to be from the same original image. VCS share with transparent pixels and pixels from the cover images. MSVCS by using halftoning techniques, and hence can treat gray-scale input share images. Embedded MSVCS encode a secret image, the dealer takes gray-scale original share images as inputs, and converts them into covering shares which are divided into blocks of sub pixels.

The stacking results of the qualified shares are all black images, the information of the original share images are all covered. The stacking results are not necessarily to be all black images. The covering shares have the advantage it's a qualified subsets of stacked. All the information of the patterns in the original share images is covered. Hence the visual quality of the recovered secret image is not affected.

Authentication has been verified by using Hash Authentication Code algorithm. only the Authorized user (Recipient) be will able to access the image, transmitted from Sender.

To detect whether or not a digital content has been tampered with in order to alter its semantics, the use of multimedia hashes turns out to be an effective solution

4.2 SEQUENCE DIAGRAM

A sequence diagram in an Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development

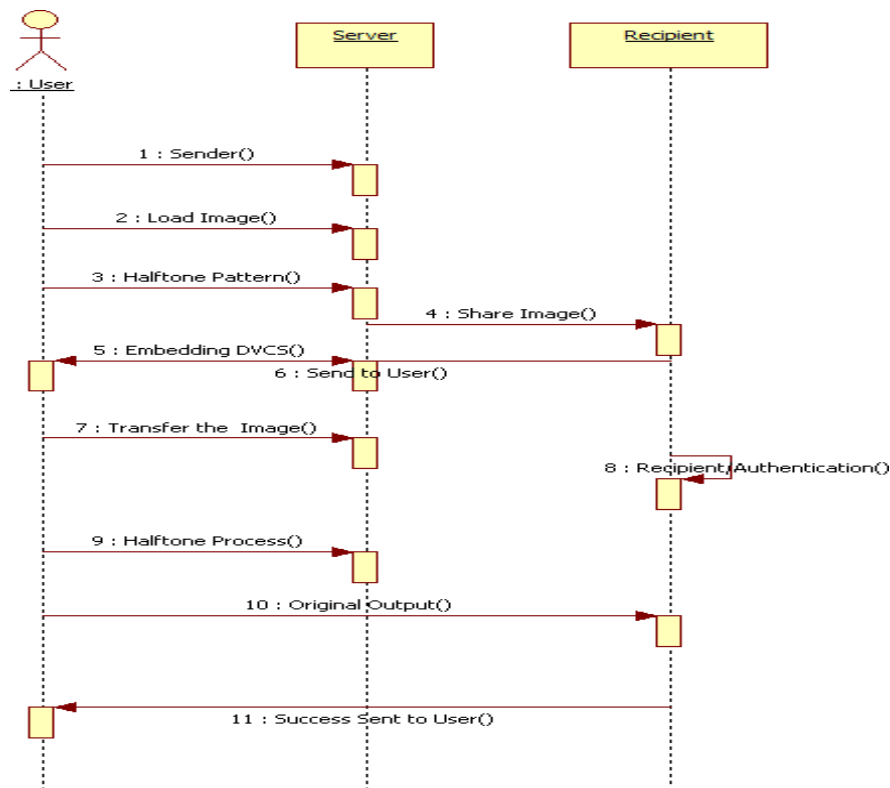


Figure 4.2 SEQUENCE DIAGRAM

Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams. In figure 4.2 the sender loads the image and the loaded image is sent to the server. The image is converted into halftone pattern. The image is then transferred to sender. The original image is then retrieved from the shared shares of transparencies

4.3 USE CASE DIAGRAM

A use case diagram is a representation of a user's interaction with the system and depicting the specifications of a use case. It portrays the different types of users of a system and the various ways that they interact with the system.

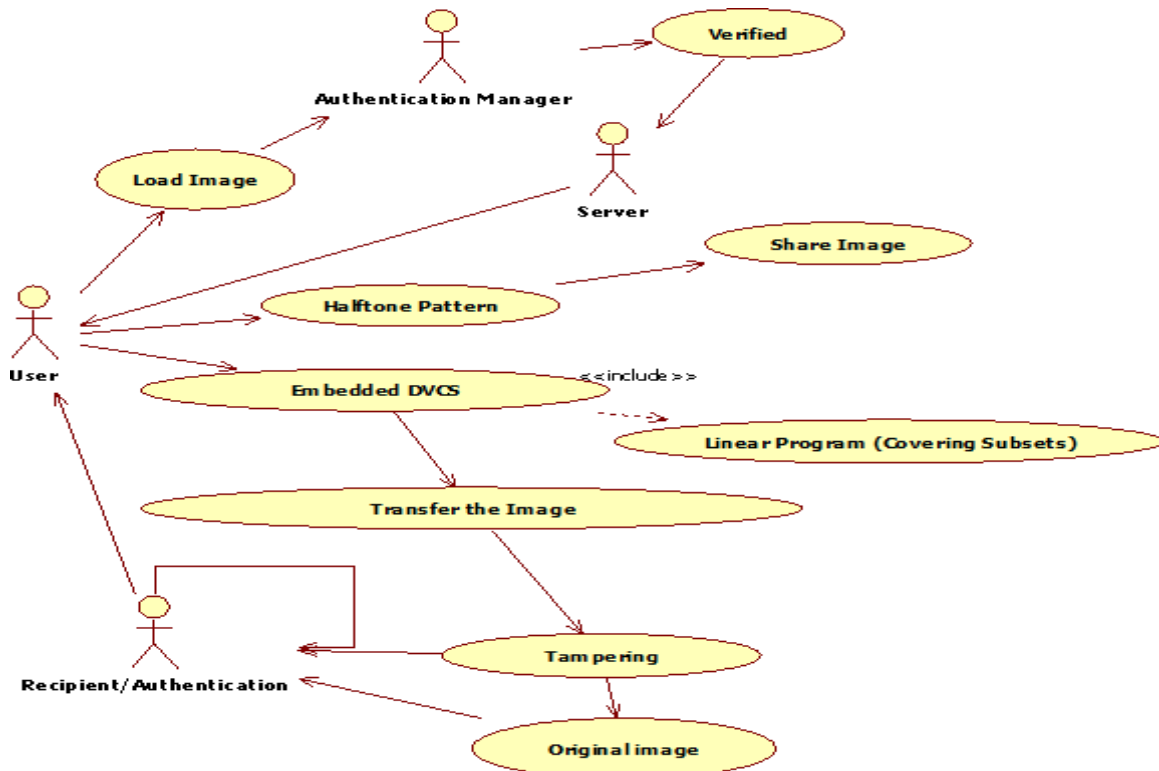


Figure 4.3 USE CASE DIAGRAM

In Figure 4.3, the first process is loading the image, then pre-processing functions are done to process all input documents into halftone Pattern. The linear program is used in the image encryption process.

4.4 STATE DIAGRAM

State diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency.

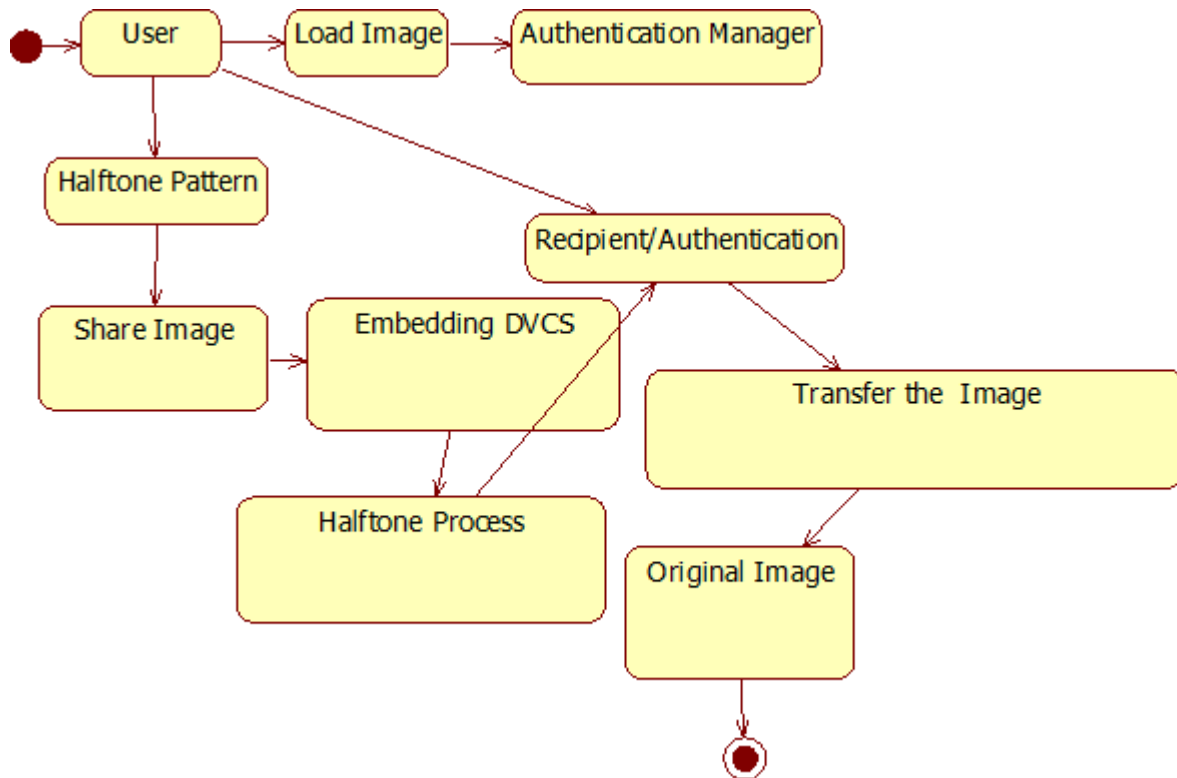


Figure 4.4 STATE DIAGRAM

4.5 COLLABORATION DIAGRAM

A collaboration diagram resembles a flowchart that portrays the roles, functionality and behaviour of individual objects as well as the overall operation of the system in real time.

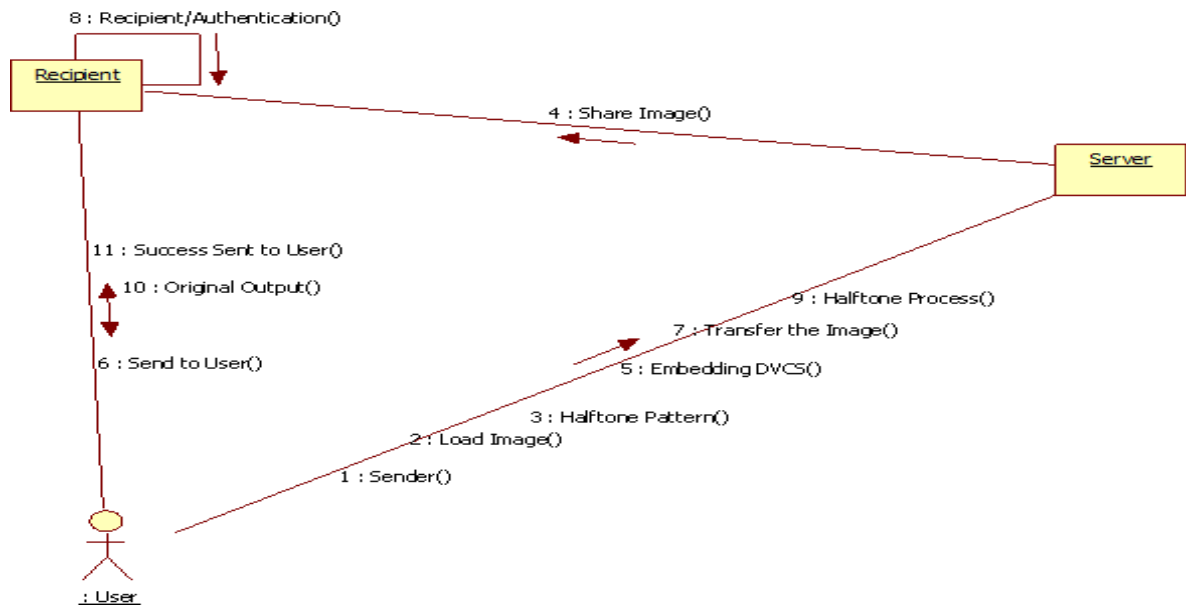


Figure 4.5 Collaboration diagram

4.6 CLASS DIAGRAM

The class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing and documenting different aspects of a system but also for constructing executable code of the software application.

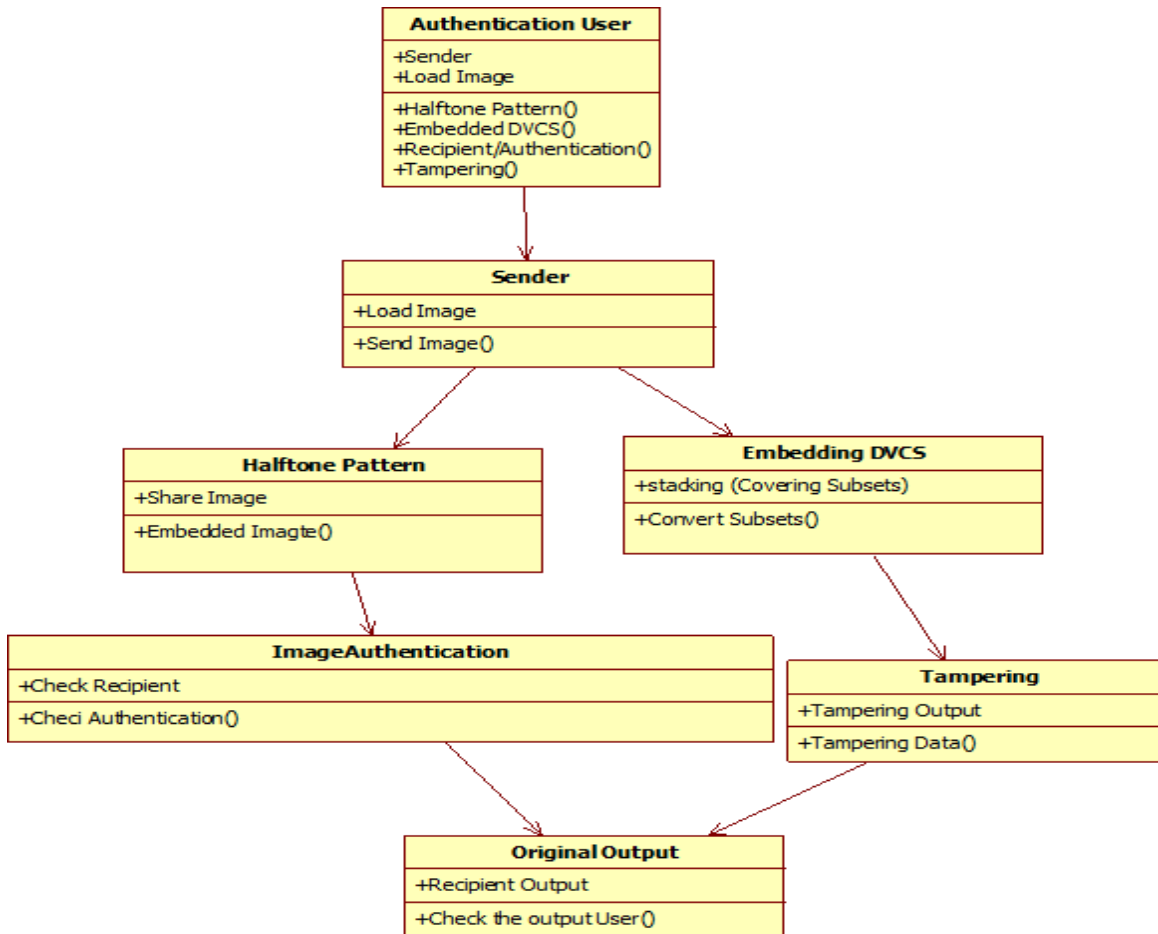


Figure 4.8 CLASS DIAGRAM

In figure 4.8 the classes used in the code is given. Sender class have the loadimage and send image methods. Halftone Pattern class have share image and Embedded image. Image Authentication class have Check Recipient methods.

CHAPTER 5

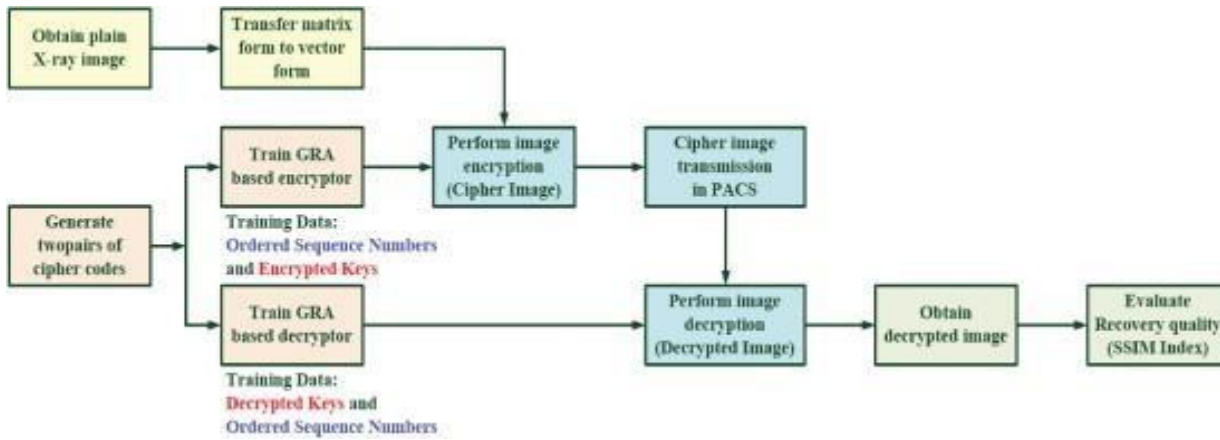
MODULE DESCRIPTION

5.1 MODULES

The modules are

1. Sender
 - a. Load Image
2. Halftone Pattern
 - b. Share Image
3. Embedded MSVCS
 - c. Linear Program (Covering Subsets)
4. Recipient/Authentication
5. Tampering

Modules Description:



GRAY SCALE IMAGE CRYPTOGRAPHY SCHEME:

The (2, 2)-VCS scheme is introduced to the basic concepts of threshold visual secret sharing schemes. In the encryption process, the secret image is divided into two shares, and each share belongs to the corresponding secret image. In the decryption process, two corresponding shares are combined together to retrieve the secret image. With (k, n) threshold visual cryptography scheme for gray level images using dithering technique, the reduction in the size of the decrypted image compared to the technique is obtained, but the quality of the decrypted image depends upon the quality of the halftone image. The halftoning is performed by the Adaptive order technique of gray-level image by using a space-filling curve to perform an adaptive variation of the cluster size. For encryption using the half-toning technique, a gray level image is changed into an approximate binary image or halftone image having pixel values 0 and 1. By considering the case of (2, 2) - VCS, the step is to divide the secret image into two shares. For decryption, the original image is reconstructed by combining binary shares.

Table 5.1-Construction of gray scale image VC

share	1 st half	2 nd half
Share 1	01010100	11011010
Share 2	10101010	11101110
Share 3	00100100	10010100

Share1 (1st half): 0 1 0 1 0 1 0 0

Share2 (1st half): 1 0 1 0 1 0 1 0

1 1 1 1 1 1 1 0 = 254

Share3 (1st half) : 0 0 1 0 0 1 0 0

Share1 (2nd half): 1 1 0 1 1 0 1 0

1 1 1 1 1 1 1 0 = 254

Share2 (2nd half): 1 1 1 0 1 1 1 0

Share3 (2nd half): 1 0 0 1 0 1 0 0

_____1 1

1 1 1 1 1 0 = 254

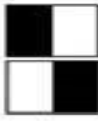
Table 5.1

Sender

User provides a secret image and outputs of Original shares image which relevant for secret . In this scheme two secret binary images were considered which were hidden into two random shares, namely share A and share B. In retrieving phase the first secretimage can be revealed by stacking the two shares, denoted by $A \otimes B$, and the second secret can be

revealed by first rotating share A by angle Θ anticlockwise.

We can satisfy with the two conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

pixel		share #1	share #2	superposition of the two shares
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

Halftone Pattern:

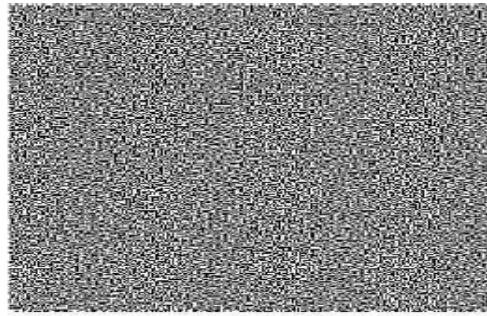
Halftoning is a print and display technique that trades area for gray-level depth by partitioning an image into small areas in which pixels of different values are purpose arranged to reflect the tone density. There are three main factors that effect these arranged pixels or dot structure, namely, the screen frequency (the number of lines perinch), the dot shape (the shape of the dots as they increase in size from light to dark), and the screen angle (the orientation of lines relative to the positive horizontal axis

We can obtain the original image with only k shares out of n shares, then all the ‘ n ’ image shares are necessarily overlaid. When all the image shares that are overlaid authenticated to be from the same original image.

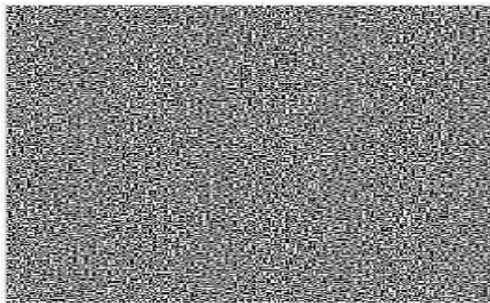
MSVCS share with transparent pixels and pixels from the cover images. MSVCS by using halftoning techniques, and hence can treat gray-scale input share images. Their methods made use of the complementary images to cover the visual informationof the share images.



(a)



(b)



(c)



(d)

By using Patterning dithering matrix makes use of a certain percentage of black and white pixels, often called patterns, to achieve a sense of gray scale in the overall point of view. The halftone is generated into share images using K-N secret sharing algorithm. The n number of transparency shares are generated and every share was saved. These shares are same size, pixel and different in transparency levels and also meaningful images

Embedded MSVCS :

Embedded MSVCS encode a secret image , the dealer takes gray-scale original share images as inputs, and converts them into covering shares which are divided into blocks of sub pixels.

Our embedded MSVCS contains three main steps:

1. Generate covering shares.
2. Generate the embedded shares by embedding the corresponding VCS into the 'n' covering shares.
3. Multiple-Secret Visual Cryptographic Schemes (MSVCS) can achieve the minimum pixel expansion and the maximal contrasts.

Integer linear program aims at the minimization of the pixel expansion under the constraints for being a MSVCS. Extended visual cryptography schemes allow the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography.

Stacking (Covering Subsets):

The stacking results of the qualified shares are all black images, the information of the original share images are all covered. The stacking results are not necessarily to be all black images.

The covering shares have the advantage it's a qualified subsets of stacked. All the information of the patterns in the original share images is covered. Hence the visual quality of the recovered secret image is not affected.

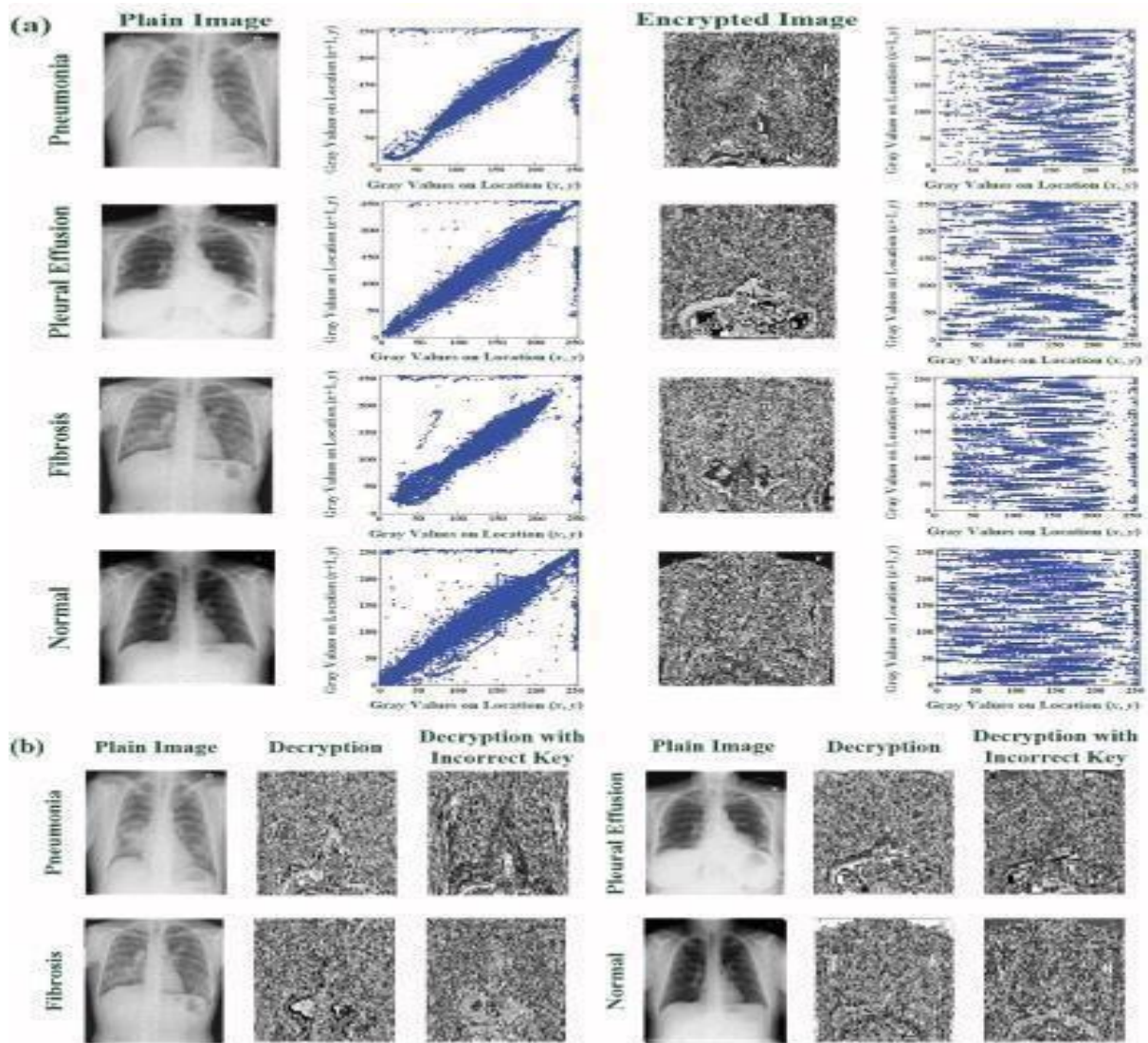
Recipient/Authentication:

Authentication has been verified by using Hash Authentication Code algorithm. Authorized user (Recipient) only be able to access the image, transmitted from Sender. Hash-based Message Authentication Code (HMAC) is a message authentication code that uses a cryptographic key in conjunction with a hash function.

Tampering:

To detect whether or not a digital content has been tampered with in order to alter its semantics, the use of multimedia hashes turns out to be an effective solution. The hash to estimate and prevent the mean square error distortion between the original and the received image.

At the cost of additional complexity at the decoder, the proposed algorithm is robust to moderate content-preserving transformations including cropping hash decoding.



Input and Outputs Modules 1

Input

To browse and select any mining full secret image

Output

To show the text-area mining full secret image

Modules 2Input

To select the number of share and number transparency of secret image.

Output

To Using Multiple secret visual cryptography techniques to generate number of transparency.

Modules 3Input

The select the number transparency and select the cover subset image.

Output

To enter the secret cryptography key and send the cover image.

Modules 4

Input

To perform destination process.

Output

To decrypt the key and the transparency from cover image.

Module 5

Input

To verify the transparency

Output

Remove the noise from transparency

Halftone Algorithm

Halftone is the reprographic technique that simulates [continuous tone](#) imagery through the use of dots, varying either in size, in shape or in spacing.

Where continuous tone imagery contains an infinite range of [colour](#) or [greys](#), the halftone process reduces visual reproductions to a [binary](#) image that is printed with only one color of ink. Halftone contact screens can be MAGENTA or GRAY in colour. TintScreen: is used in the platemaking process to create the uniform tone pattern and contains a hard dot structure that is specified by a dot percentage.

- Highlight = 5-10% in size.
- Midtone = 30-70% in size.
- Shadow = 90-95% in size
- Highlights: the whitest tonal value.
- Midtones: the gray tonal values.
- Shadows: the darkest black tonal value.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENTS

6.1 CONCLUSION

We established an efficient construction of n -MSVCS using the skill of linear programming in this paper. The object function aims at minimizing the pixel expansion subject to the constraints satisfying the region incrementing requirements. Unitmatrices are introduced as the building blocks and the numbers of the unit matrices chosen to form the basis matrices of n -MSVCS are set as the decision variables. A solution to these decision variables by our linear program delivers a feasible set of basis matrices of the required n -MSVCS with the minimum pixel expansion. The pixel expansions and contrasts derived from our n MSVCS are better than the previous results. Since no construction method has ever been reported in the literature, our linear program formulation for n -MSVCS is novel and innovative from both the theoretical and practical points of view. The contrasts of different secret regions can also be designated in the constraints. This enhances the adaptability and flexibility of our MSVCS in practical applications.

6.2 FUTURE ENHANCEMENTS

Embedded MSVC has many specific advantages against different well-known schemes, such as the fact that it can deal with gray-scale input images, has smaller pixel expansion, is always unconditionally secure, does not require complementary share images, one participant only needs to carry one share, and can be applied for general access structure. Furthermore, our construction is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares.

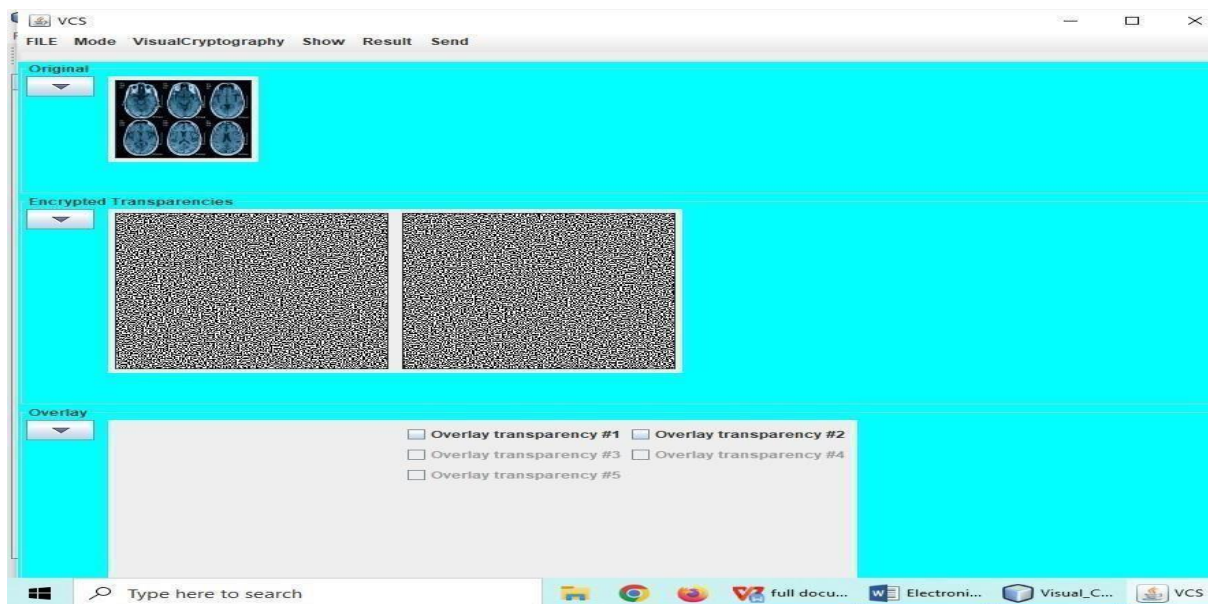
APPENDIX I

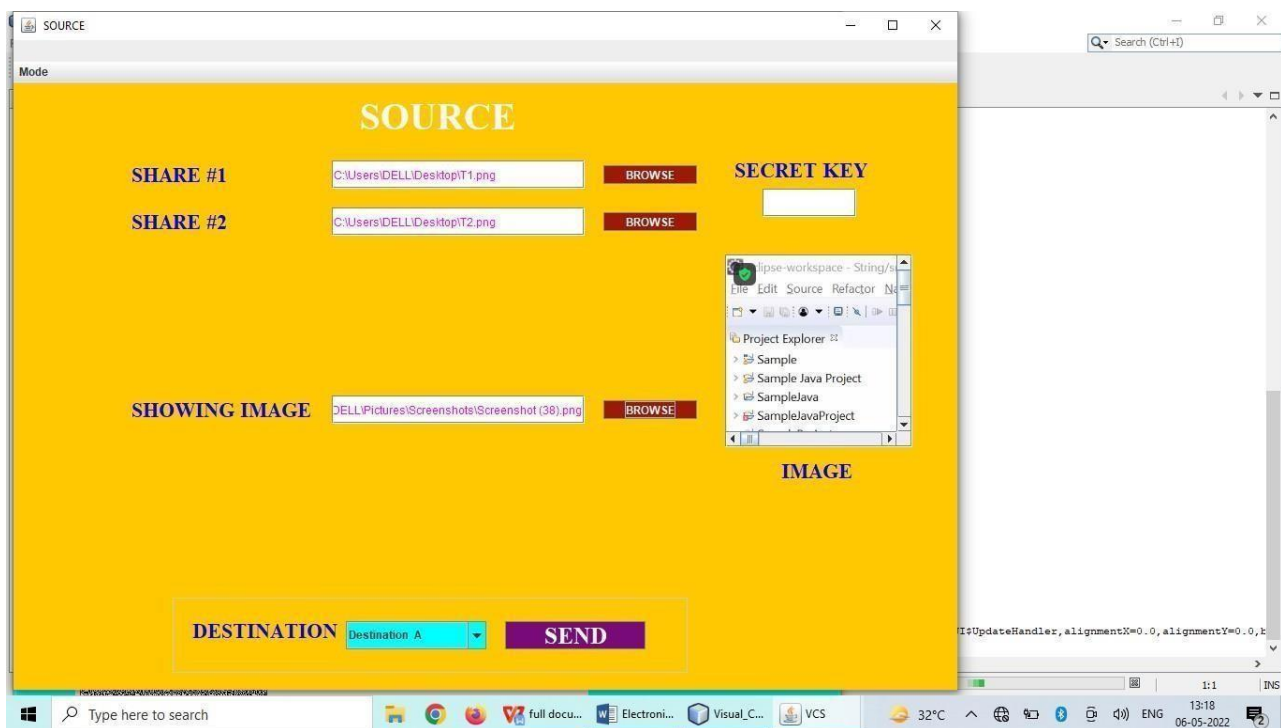
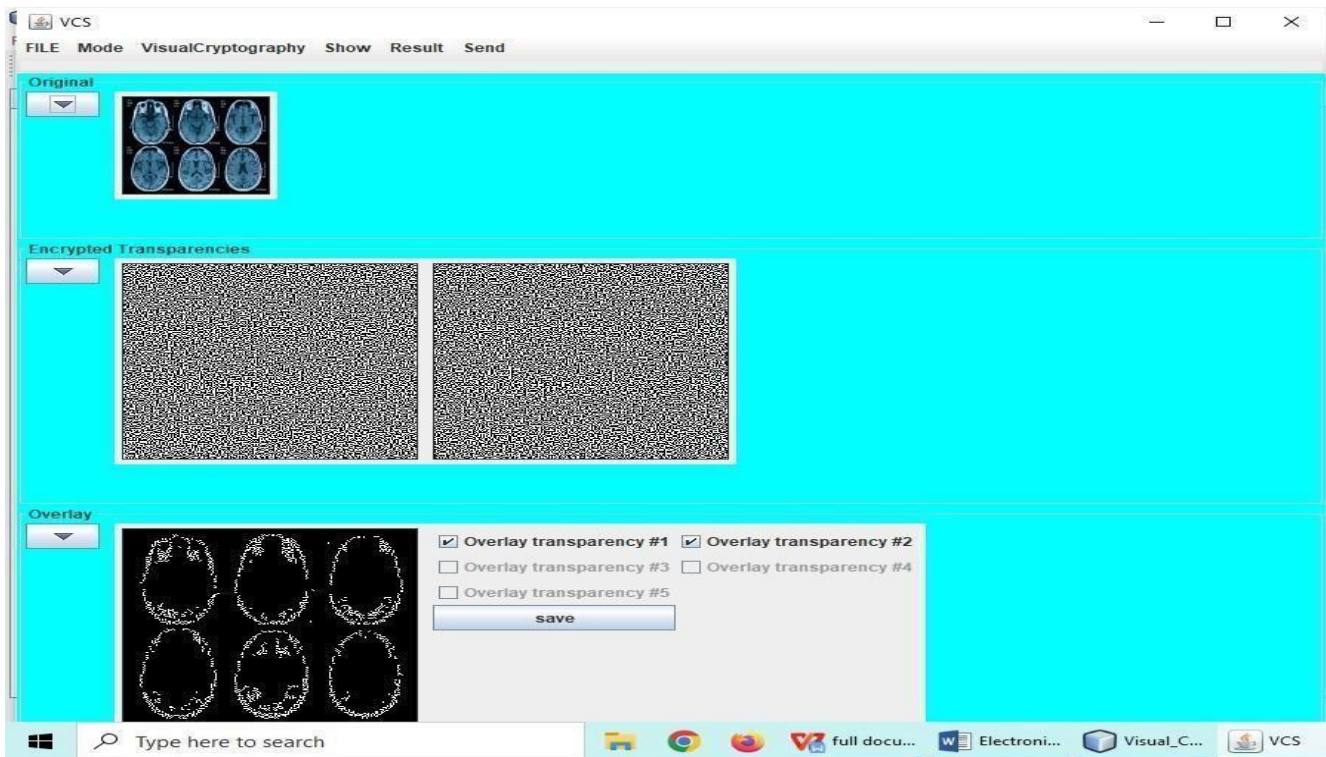
Sample Coding

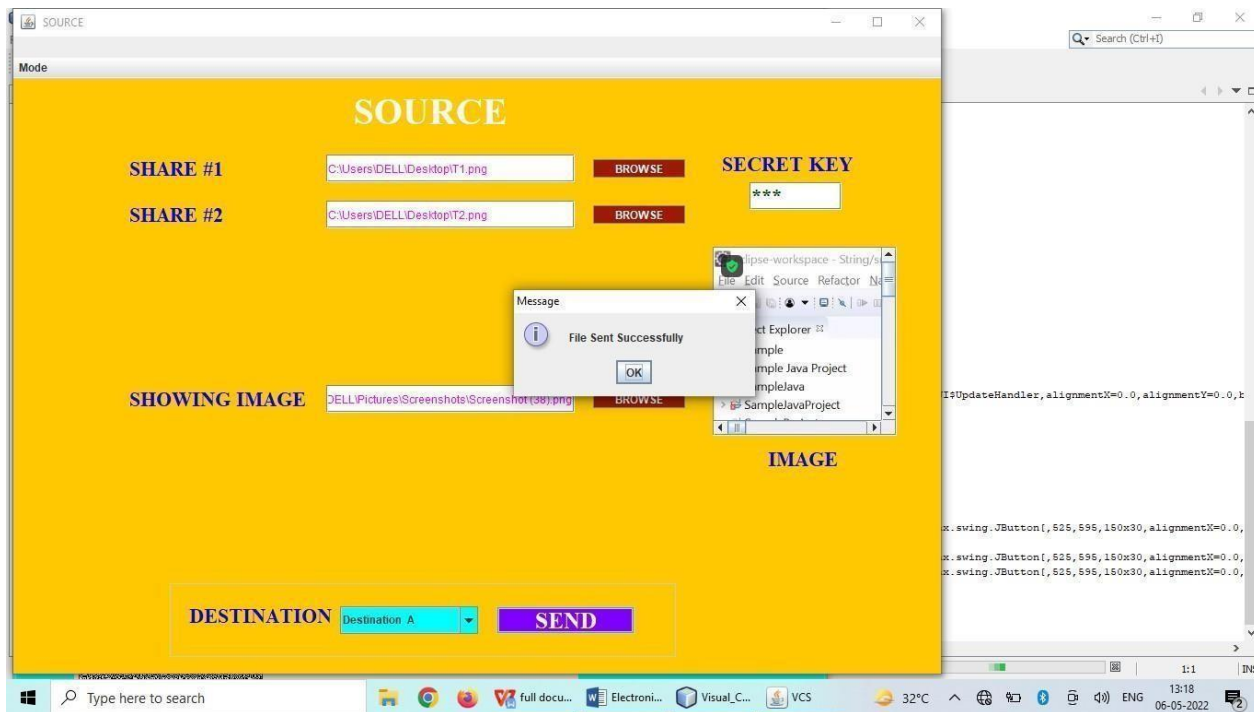
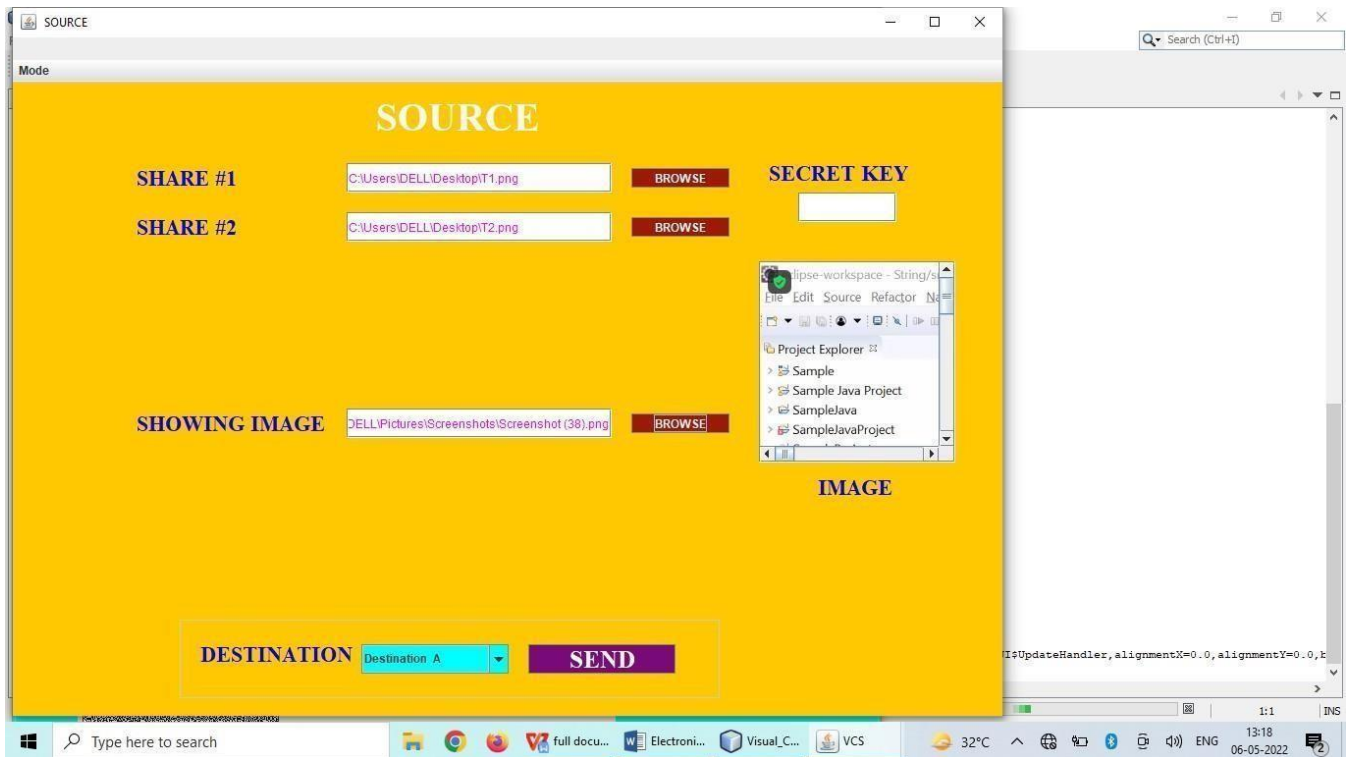
SOURCE CODE

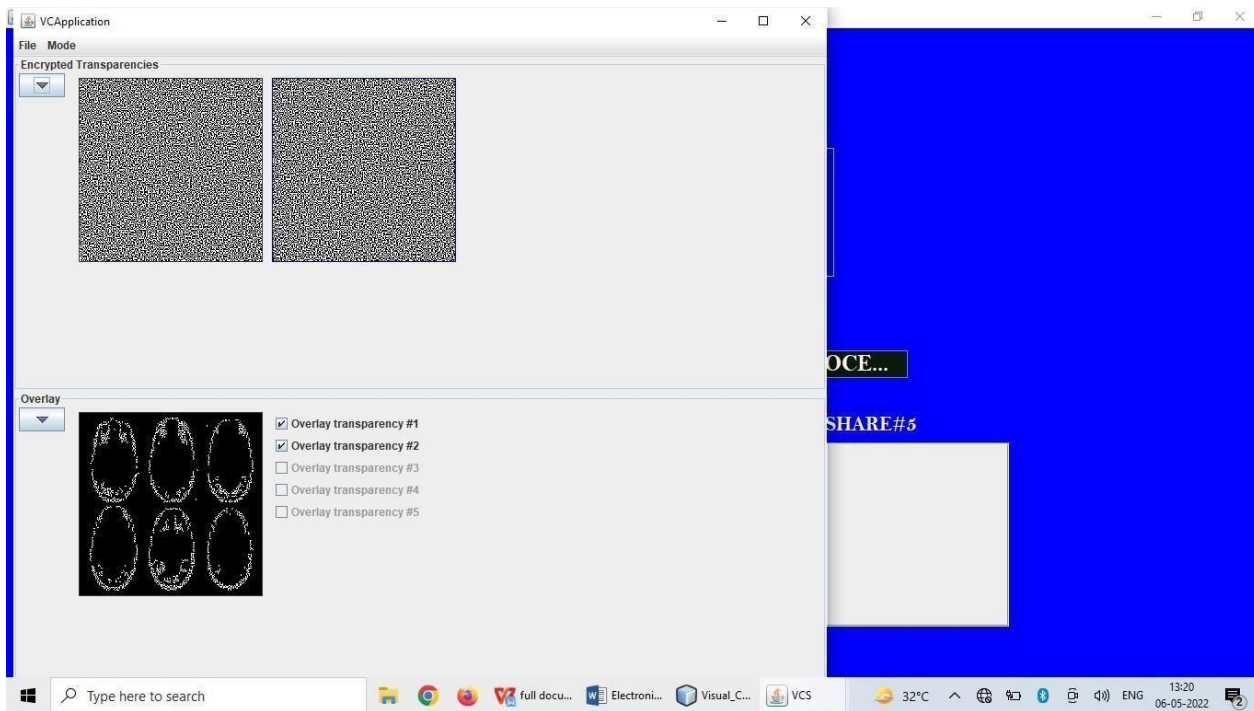
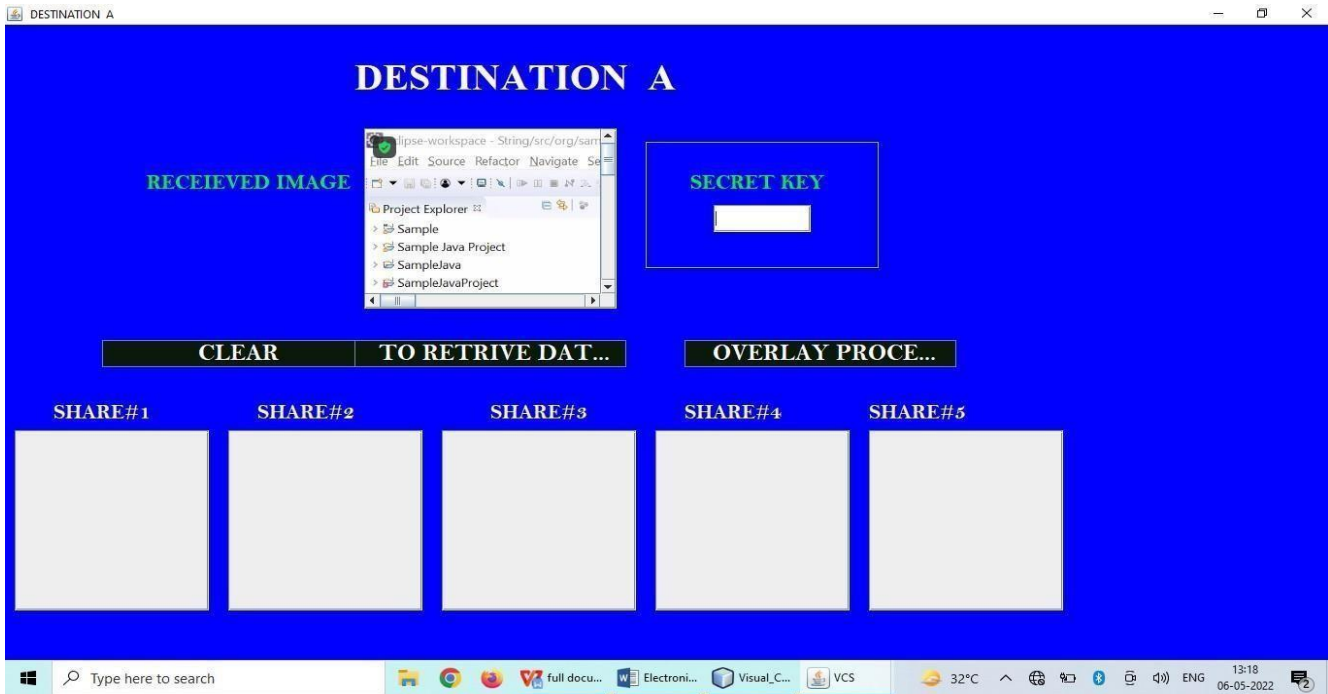
```
import javax.swing.JApplet;                import javax.swing.JFrame;                import java.awt.Dimension;
import java.awt.event.ActionEvent;          import java.awt.event.ActionListener;    import java.awt.event.ItemEvent;
import java.awt.event.ItemListener;         import java.io.File;    import java.io.IOException;    import java.net.URL;
import javax.swing.AbstractButton;          import javax.swing.JEditorPane;          import javax.swing.JFileChooser;
import javax.swing.JFrame;                  import javax.swing.JOptionPane;          import javax.swing.JScrollPane;
import javax.swing.event.HyperlinkEvent;    import javax.swing.event.HyperlinkListener    ;
import javax.swing.filechooser.FileFilter; import anon.util.ResourceLoader; /** AppletListener for the VCApplet to
listen on Actions and ItemState-Events * @author Boßle Johannes */ 33 public class VCAppletListener
implements ActionListener, ItemListener, HyperlinkListener { /** the applet which called this VCAppletListener
*/ VCAppletm_applet; /** flag to see if there are loaded encrypted transparencies*/ booleanm_LoadEncFoil = false;
/** creates a new VCAppletListenerObject * * @param applet - the applet to listen to */
public VCAppletListener(VCApplet applet){ m_applet = applet; } /** creates a filechooser to select images to load
* * @param desc - description to display * @param loadEnc - true if encrypted foils are loaded, false otherwise *
@return - JFileChooserObject with filter, description,... */ private JFileChooser getFileChooser(String desc,
boolean loadEnc){ JFileChooser jfc = new JFileChooser(desc); jfc.setFileFilter(new FileFilter(){ public boolean
accept(File f){ boolean ret = false; if (f.isDirectory()) { return true; } if (ImagePanel.extension(f)!= null){ ret = true;
34 } return ret; } public String getDescription(){ return "*.gif, *.png"; } }); jfc.setAccessory(new
ImagePreview(jfc)); return jfc; } public void actionPerformed(ActionEvent evt) { m_applet.setEncTFText(); String
actionCommand = evt.getActionCommand(); try{ //File if (actionCommand == (m_applet.loadItem.getText()) ||
actionCommand == m_applet.loadButton.getActionCommand()) { JFileChooser jfc = this.getFileChooser("load a
new original image",false); if(jfc.showOpenDialog(m_applet)==JFileChooser.APPROVE_OPTION){
m_applet.m_fileImage = jfc.getSelectedFile(); m_applet.m_dispatcher.loadImage(m_applet.m_fileImage);
m_applet.inputPanel.setVisible(false); m_applet.inputPanel.setVisible(true); m_applet.updateMenu();
m_applet.enableFunctionsAfterEncrypt(false); m_applet.inputPanel.validate(); } 35 } } //Show else
if(actionCommand == m_applet.zoomButton.getActionCommand()){ m_applet.m_dispatcher.zoom(); }else
if(actionCommand == m_applet.show1Item.getText() actionCommand ==
m_applet.show1Button.getActionCommand()){ m_applet.m_dispatcher.getEncCanvas(0);
m_applet.setEncTFText(); m_applet.show1Button.setBackground(m_applet.SELECTEDCOLOR); || }else
```

APPENDIX II SCREENSHOTS









1REFERENCES

- [1] A. Adhikari and S. Sikdar, “A new $(2,n)$ -visual threshold scheme for color images,” in *Proc. 4th Int. Conf. Cryptol.*, Dec. 2005, pp. 148–161.
- [2] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Visual cryptography for general access structures,” *Inf. Comput.*, vol. 129, no. 2, pp. 86–106, Sep. 1996.
- [3] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, “Extended schemes for visual cryptography,” *Theoretical Comput. Sci.*, vol. 250, pp. 143–161, Aug. 2001.
- [4] C. Blundo, S. Cimato, and A. De Santis, “Visual cryptography schemes with optimal pixel expansion,” *Theoretical Comput. Sci.*, vol. 369, nos. 1–3, pp. 169–182, Dec. 2006.
- [5] C. Blundo, A. De Bonis, and A. De Santis, “Improved schemes for visual cryptography,” *Des., Codes Cryptogr.*, vol. 24, no. 3, pp. 255–278, Dec. 2001.
- [6] C. Blundo, P. D’Arco, A. De Santis, and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” *SIAM J. Discrete Math.*, vol. 16, no. 2, pp. 224–261, 2003.
- [7] C. Blundo and A. De Santis, “Visual cryptography schemes with perfect reconstruction of black pixels,” *J. Comput. Graph.*, vol. 22, pp. 449–455, Jan. 1998.
- [8] C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” *J. Cryptol.*, vol. 12, no. 4, pp. 261–289, Sep. 1999.

- [9] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, “Self-verifying visual secret sharing using error diffusion and interpolation techniques,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 790–801, Dec. 2009.