Multi-Pixel Visual Cryptography For Coloring Pages Using Meaningful Shares

[1]Sethuram V, [2]Sirajudeen S, [3]Krishna Teja R [4]Saikrishna P

[1]Student(RA1411003020030), [2]Student(RA1411003020026), [3]Student(RA1411003020042) [4] Student(RA1411003020026)
[1]B.Tech Computer Science and Engineering,
[1]*SRM Institute of Science and Technology, Ramapuram campus, Bharathi Salai, Chennai 600089.*
Tamil Nadu, India

Abstract : *This paper describes our first research experience in Visual Cryptography using AES algorithm by using open-source software tools such as Java(Eclipse), My Sql and etc .Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images/layers are required to reveal the information. Using secret sharing concepts, the encryption procedure encrypts a secret image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an unsecured communication channel. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography. Any visual secret information (pictures, text, etc) is considered as image and encryption is performed using simple algorithm to generate n copies of shares depending on type of access structure schemes. The simplest access structure is the 2 out of 2 scheme where the secret image is encrypted into 2 shares and both needed for a successful decryption.*

IndexTerms - Visual-cryptography,*Toning Process,Half-Toning ,XOR,OR.*

I. INTRODUCTION

The recent market requirement for transfer data is changed from text to images. Transfer of Images through network is no more secure. The transferred images are manipulated in the network by hackers. Confidential Images has no means to be secure anymore in the network. In the traditional visual cryptography schemes, only one piece of image was encoded during encryption. Due to the capacity of encrypted information, these schemes have few applications. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent

sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

II. LITERATURE SURVEY

1. *Existing System:*

Encrypting an image was initially done by random grids (RGs) which was introduced by Kafri and Keren in 1987. A binary secret image is encoded into two noise-like transparencies with the same size of the l secret image, and stacking of the two transparencies reveals the content of the secret Image as such. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices. The recent studies include the RG for color image. Since Rg Scheme was not based on matrices the encryption technique was as such reduced to a particular set of codes and these were prone to be hacked much easier

I.I Issues in Existing System:

Images are manipulated by the attackers in the network. Confidential Images has no means to be secured when they are transmitted over the network. In the traditional visual cryptography schemes, only one piece of image was encoded during encryption. And each of the shares that are generated was shown as a disorganized image. Due to the capacity of encrypted information, these schemes have few applications and because of the disorganized image share, they are easily suspected by hacker. The generated shares are not meaningful. This project proposes a selective encryption technique in wavelet domain for conditional access systems. The encryption is applied only to a subset of multimedia data stream rather than the multimedia data in its entirety to save the computational time and computational resources. The Proposed System method scans the original image in the determined order and, moreover, encrypts the SCAN string by using commercial crypto systems. Since the illegal users cannot obtain the correct SCAN string, the original image is therefore secure. There is no image compression in this method. Therefore, the size of the image is very large, and thus it is inefficient to encrypt or decrypt the image directly.

2. *Proposed System:*

Visual Cryptography for color images to generate two meaningful shares. Some filters are proposed for better visual quality of recovered image.The input image is decomposed into three channels of Cyan, Magenta and Yellow by using equation. Error Diffusion produces halftone of much higher quality than other halftone. Halftone is applied on each monochrome image. It is applied on each halftone channel to generate shares. There will be two shares for each halftone.A multi-pixel non-expanded scheme for color images introduced which can encode more than one pixel for each run resulting same size of shares as secret image.A new simple watermarking algorithm is proposed to generate meaningful shares. Decryption is achieved by stacking the shares. In case of black pixel, overlaying two rows of M1 results in four black bits, and reveals the information, where asfor the white pixel, stacking the two rows of M0 results in two black and two white bits, and thus introduces noise.

II.1. Advantages of Proposed System

1. Simple to implement
2. Decryption algorithm not required (Use a human Visual System). So a person unknown to cryptography can decrypt the message
3. We can send cipher text through FAX or E-MAIL.
4. Lower computational cost since the secret message is recognized only by human eyes and not cryptographically computed.

III **SYSTEM ANALYSIS AND DESIGN**

1 Introduction

A Visual Cryptography is usually performed to generate a picture which has an encoded message in it. Thus making the transmission of important messages in much secure way.The paper describes two methods of half toning being used for the transmission of the messages.

2 Analysis of the problem

1. *Single Toning for message Transmission*

The message that is being transmitted usually uses a single Toning and usage of a single color for the transmission of the images. The transmission is usually done by using the conversion of the image into black and white thus a change is done to overcome this issue

2. *The top common issues in Encoding an image:*

The message needs to be converted into a water mark thus making it as another share and avoiding the loss of Message throughout the transmission

3. System architecture:

The architecture mainly describes the various usage of filters that is used to split an image into diffrent colors thus making it possible for the encoding to take place two different types of half toning is done thus making it much secure in the transmission of the image the public key and private key are generated and added to the particular image.

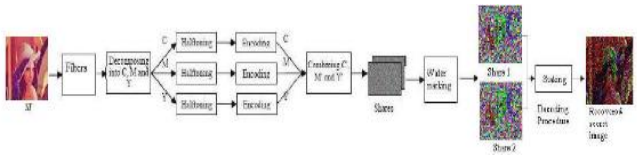

Figure 1: System Design

IV. MODULE DESCRIPTION

1 Introduction

Our complete project deals with the different modules based on the working. The workings are based on the design and implementation. The Multi-Pixel Visual Cryptography for Coloring pages consists of various modules as described below,

1. Security And Login Module
2. Encoding the Image
3. Decoding the Image
4. Verification of Images
5. .User Interface Manual

2 IMPLEMENTATION

Overview:

1. *Security And Login Module:* This module deals with ensuring that only authorized users can access to this application. A database with user-id and password is used to validate the User entry. The input user-id is validated for a minimum of four characters. The application the opens into the application screen on validation.

2. *Encoding The Image:* This system uses the Secret Sharing Scheme, which is a method for sharing a secret among a set p of participants. The secret is encoded into n pieces called shares eachof which is given to a distinct participant. Certain qualified subsets of participants can recover the secret by pooling together their information, whereas forbidden subsets of participants have information on the secret. The specification of the qualified sets and the forbidden sets is called access structure. A special kind of secret sharing schemes are Visual Cryptography Schemes (VCSs),that is, schemes where the secret to share is an image and the shares consist of xeroxed transparencies which are stacked to recover the shared image. In this project we analyze the relationship between secret sharing schemes and VCSs, focusing our attention on the

amount of randomness required to generate the shares. We show how to transform a secret sharing scheme for a given accessness of the original scheme. An important consequence of this transformation is that lower bounds on the randomness of visual cryptography schemes apply to general secret sharing schemes. Our randomness preserving transformation has also been applied to derive a new upper bound on the randomness k, n threshold VCSs which dramatically improves on the previously known bounds. All VCSs obtained by applying our randomness preserving transformation allow a perfect reconstruction of blackpixels.

3. *Decoding The Image Module* This module just performs the operation that are done in the encoding module thus separating the two shares one on one and delivering the output message.
4. *Verification of the Image Module:* This module is used in verifying the contents of the message and the implementation of the algorithm whether it is successful or not.
5. *User Interface Module:* This module speaks about the user interface that is done for the easier implementation of the user and the description of the usage is also specified.

1. *USE CASE DIAGRAM: Description***:** the use case diagram gives an explained process of how the Visual cryptography is being done .

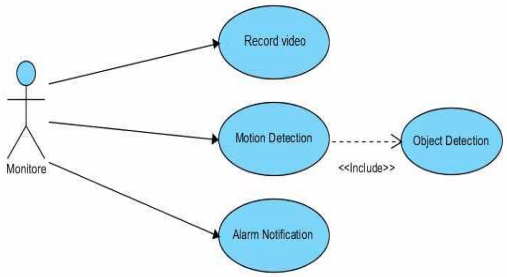

Figure 2: Use Case Diagram

CODE:

For executing the main program install java and implement the program from IDE

Right click and run the program as such

Screenshots:

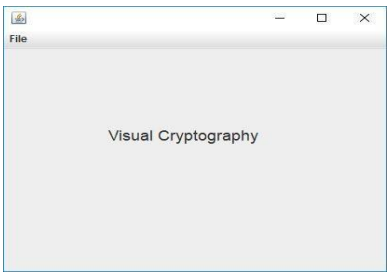

Figure 3: Home Page

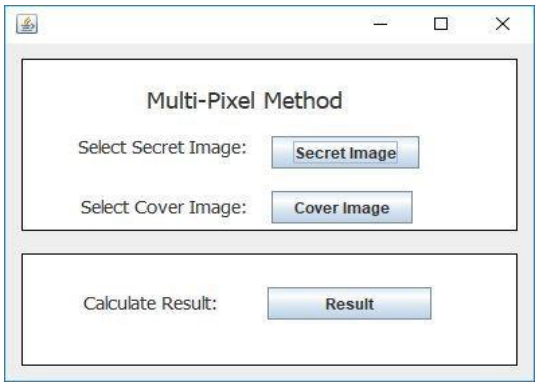

Figure 4: Final Output

V. CONCLUSION AND FUTURE WORK

The project was done successfully with all the requirements. The future work is improving the algorithm and making the work more optimize for use.

VI. REFERENCES

1. www.google.com.
2. www.wikipedia.com
3. www.w3schools.com
4. www.instructables.com