CSE 4003

CYBER SECURITY

IMAGE CRYPTOGRAPHY IN SOCIAL MEDIA

J-COMPONENT PROJECT REPORT

Submitted by:

18BCE2481 DHANANJAY KAPAR

18BCE2484 SHUBHAM SHAH

18BCE2491 SHADAB ALAM

Under the guidance of

DEEPIKA S

In partial fulfillment for the award of the degree of

B.Tech.

in

COMPUTER SCIENCE AND ENGINEERING

INDEX

ABSTRACT

Services such as Online transactions and Social networking are an increasing target demographic for customers. In this project we use visual cryptography for transactions and network security. Simultaneously, there has been an increasing risk for protection against hacker's use are need of unfair gain by exploiting such systems. The end users are need to protected from such users and their privacy is to be maintained.

Visual cryptography is such a technique in which an image is ciphered into random images (which cannot be read) when paired with secret images such that when they are paired appropriately under a particular algorithm, the plaintext can be read.

Our basic objective in the project is to encrypt images appropriately in social media. As social media is a vast platform, millions of users share their images online and the content isoften not secured resulting in large risk of cyber abuse and misuse. This can also be applied in banks and military bases, where sensitive information is transferred and encryption if data is necessary.

But visual cryptography has its range of disadvantages: due to the fine resolution as well as printing noise, it is not very quick to do exact superposition. In addition, many visual cryptography applications have to print shares on paper on which the share needs to be scanned.
Noise can also be introduced by the print and scan system, which can make alignment difficult.

1.INTRODUCTION

Two Greek terms meaning "code prose" are used to extract the expression cryptography. Through rearranging and deleting the original text, cryptography is the method of scrambling the original text, organizing it in an almost unreadable way. Visual cryptography is a crypto graphic technique that facilitates encryption of visual content (images, text,etc.) in such a way that decryption can only be achieved by reading visual information.Visual cryptography, degree associated rising cryptography technology, uses the characteristics of human vision to rewrite encrypted photos.

Visual cryptography, associated with the growing technologies of cryptography, uses human vision features to rewrite encrypted images. Visual cryptography offers secure digital transmission that is only used once. Unlike the complex algorithm used in other classical cryptography, Visual Cryptographic is one of the latest techniques that provide information security and uses the basic algorithm.

EXISTING SYSTEM AND ITS DRAWBACKS

- Although there are encryption systems present already which serve the purpose of visual encryption, the technique we aim to employ provides a unique way of encrypting an image by breaking it down into not one, but two noisy images, one generated at random and one that holds the cipher message thus making it even more difficult for attackers to decipher.
- The drawbacks of the existing system are that they use a single algorithm for encrypting the file and once the algorithm is cracked by attackers, they'll be able to retrieve all the files that are yet to be shared, while if we generate both a random ciphered image along with a secret image, knowing the algorithm alone is not enough to decipher the yet to be shared files.

2.LITERATURE SURVEY

[1] Jing Qiu and Ping Wang, " Image encryption and authentication scheme", IEEE, Computational Intelligence and Security (CIS), 2011 Seventh International Conference, 3-4 Dec. 2011, 784 – 787.

The scheme was proposed by Jing Qiuand ping Wang [5].The method presents a fast image encryption and authentication scheme. In the scheme, a 512 bit message authentication code (MAC) of the plain image is converted into 64 bytes and these 64 bytes are replaced with the image pixels in some way. Replaced pixels are then embedded into the image by reversible data embedding technique. Then the embedded image is masked by using the pseudo random sequence in feedback mode. The MAC provides authentication and also provides some encryption to the image. The scheme provides encryption as well as authentication to the image the embedded MAC plays important role in determining the integrity of the image.

[2] R. Soni, A. Johar and V. Soni, "An Encryption and Decryption Algorithm for Image Based on DNA," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013, pp. 478-481, doi: 10.1109/CSNT.2013.105.

In 2013, a novel colour image encryption algorithm based on DNA sequence operation and hyper chaotic system was proposed[10] . In this paper chen's hyper-chaotic system is used to scramble the position of the pixels then the colour image is converted into three matrices for R, G and B which are transformed into binary matrices and DNA addition operation is performed .The experimental results and the security analysis will shows that algorithm has good encryption effect, larger secret key space and high sensitivity to the secret key.

[3] Kushwah, K. and S. Shibu. "New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique." (2013).

In this paper, a new image encryption algorithm is proposed. It is already known that security of an algorithm depends on the length of the key. this means that longer keys will always support good security features. The proposed algorithm uses 128- bit key which provided too much security for the proposed algorithm. To access original key or crypto analysis of the proposed key is required 2128 time to break the key which is almost impossible for any hacker. There is no chance to generate floating point error because no such types of mathematical formulas have been applied on the proposed algorithm. The correlation co-efficient as well as their entropy values for the proposed algorithm were calculated.

[4] Saraf, K., Vishal P. Jagtap and A. Mishra. "Text and Image Encryption Decryption Using Advanced Encryption Standard." (2014).

This paper implemented text and image encryption and decryption using AES. Features of data are depends on its types. Therefore same encryption technique cannot be used for all types of data. If the Images have large data size and also have problems with real time constrain hence similar method cannot be used to protect images as well as text from unauthorized access. Few variations in method AES can be used to protect image as well as text.

[5] Pakshwar, R. & Trivedi, Vijay & Richhariya, V.. (2013). A survey on different image encryption and decryption techniques. Int Journal of Computer Science and Information Technologies. 4. 113-116.

This paper presented a survey of over 25 research papers dealing with image encryption techniques that scrambled the pixels of the image and decrease the correlation among the pixels, which lowers correlation among the pixel and produces the encrypted image. A survey of different existing image encryption and decryption techniques was given. Additionally, the paper focused on the functionality of Image encryption and decryption techniques.

3.PROPOSED WORK

In certain cases, even with incredible developments in computer technology, using a computer to decode hidden images is difficult. In these cases, one of the most convenient and effective methods for hidden recovery is the human visual system. Moni Naor and Adi Shamir pioneered Visual Cryptography in 1994.

They come up with a visual hidden sharing scheme where an image is split or divided into nshares such that the image can only be decrypted by someone with all n shares, thus no information about the original image can be revealed by someone with any n-1 shares. Each share is printed on a separate transparency (which serves the secret key purpose) and decryption is done by overlaying the shares when the original image is seen when all n shares are overlaid.

Visual Cryptographic is one of the new techniques which provide information security and uses the simple algorithm unlike the complex one used in other traditional cryptography.

This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex computation or algorithms. This is known as (k,n) VCS model where k represents minimum no of shares needed to decrypt the secret image and n is the total number of shares generated by the visual cryptographic scheme.

Hence, the whole Visual cryptographic process can be summarized as:

- Plaintext (in the form of image)
- Encryption (creating shares)
- Channel (Fax, E-mail)
- Decryption (Human Visual System)

MODULAR DESIGN

1. **Input Verification Module** – We must first ensure that the input image(message) tobe encrypted is of a valid size, dimension, etc., before beginning the encryption process

2. **Load Module**- The input message/image is loaded in this module.

3. **Message Image Preparation** - If the image was not of a suitable size, this modulewill process it as resize it appropriately. before encryption

4. **OTP Module** - The secret image with one-time validity is generated by this modulewith random pixelizations (onetime pad algorithm)

5. **Image Ciphering Module** - The input image is ciphered by shuffling pixels, adjustingto the secret image appropriately.

6. **Image Decryption Module**- The main function integration with PIL is carried out hereto use the secret image to decipher the message/image that has been encrypted.

Innovative Ideas

- Contrast improvement
- Share size improvement
- Pixel expansion
- Ability of sharing single/ multiple secret images
- Efficiency
- Security
- In order to improve the quality of decrypted images, inverse half toning can beapplied.

Architecture Diagram-

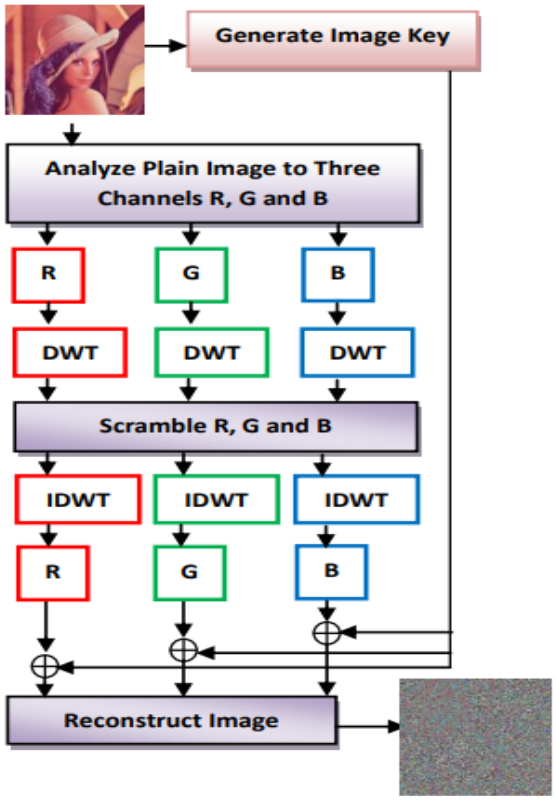


Figure: Proposed Encryption Algrithm

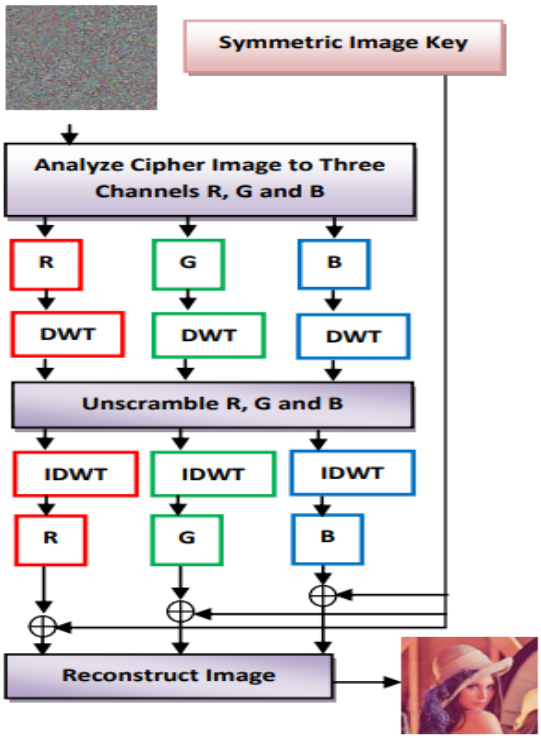


Figure: Proposed Encryption Algorithm

4. IMPLEMENTATION

Algorithms Used:

- Input Image Verification Algorithm Image (Message) Encryption Algorithm
- Random Image Key Generation Algorithm (OTP)
- Ciphered and Key Image Alignment (Decryption)

TOOLS:

Encryption:

- IDLE (Integrated Development Environment for Python)
- Python 3.4
- Python Image Library (PIL)
- Pillow (PIL fork) 5.1.0

Decryption:

- Transparent sheets for dem

APPLICATIONS OF VISUAL CRYPTOGRAPHY:

- Biometric security
- Watermarking
- Steganography
- Remote electronic voting
- Bank customer identification – Bank sends customer a set of keys in advance – Bank web site displays cipher – Customer applies overlay, reads transaction key – Customer enters transaction key

ADVANTAGES OF VISUAL CRYPTOGRAPHY:

- Simple to implement Decryption algorithm not required (Use a human Visual System). So a person unknown to cryptography can decrypt the message. We can send cipher text through FAX or E-MAIL. Lower computational cost since the secret message is recognized only by human eyes and not cryptographically computed.
- Simple to incorporate. (Use a human visual system) No decryption algorithm needed. So the message can be decrypted by a person unknown to cryptography. We can send encrypted text via FAX or E-MAIL. Lower computational cost because only human eyes are known and not cryptographically calculated for the hidden message.

DISADVANTAGES OF VISUAL CRYPTOGRAPHY:

- The contrast of the reconstructed image is not maintained.
- Perfect alignment of the transparencies is troublesome.
- Due to pixel expansion the width of the decoded image is twice as that of the original image.
- Leads to loss of information due to change in aspect ratio.
- Additional processing is required for coloured images. The first two main tasks are asfollows:
    - An image to be to be kept as a secret is taken to produce a ciphered image which will look completely random.
    - A secret image (also random) which can be combined appropriately with the ciphered image is produced. This should be allowed to use only once so as toprevent easy deciphering.
- The desired receiver now observes the deciphered image(darker) by combining the ciphered and one-time valid secret image. Using one-time-pad algorithm forbids reuse of the secret image, this one-time validity helps make the cryptography impenetrable and safe from attackers.
- Appropriate alignment can be done by printing the ciphered and the secret image on transparent sheets or digitally. In this project we execute a combination of three codes, one to digitally cipher the image, a code to generate a one-time secret key and a code to align the random key image with the encrypted image to decipher it at the receiver's end.

CODE-

Main.py

```
import os
import sys
from PIL import Image

from generate_image import combine_color, generate_ciphered_image, generate_decrypted_image,
generate_secret, separate_color


def load_image(name):
    return Image.open(name)

def main(argv):

    input_image_name = str(argv[1])
    message_image = load_image(input_image_name)

    color_images = separate_color(message_image.convert("RGB"))

    # color_images[0].save("R_image.png")
    # color_images[1].save("G_image.png")
    # color_images[2].save("B_image.png")

    # combined_image = combine_color(color_images)
    # combined_image.save("Decrypt_"+input_image_name)

    # sys.exit(0)

    secret_image = generate_secret(message_image.size)
    secret_image.save("images/secret_"+input_image_name)

    #ciphered_image = generate_ciphered_image(secret_image,message_image)

    ciphered_color_images = []
    RGB_msg = ["R","G","B"]
    for i in range(3):
        ciphered_color_images.append(generate_ciphered_image(secret_image,color_images[i]))
        ciphered_color_images[i].save("images/ciphered_"+RGB_msg[i]+"_"+input_image_name)


    ciphered_image = combine_color(ciphered_color_images)
    ciphered_image.save("images/ciphered_"+input_image_name)
```

```
    decrypted_images = []

    for i in range(3):
        decrypted_images.append(generate_decrypted_image(secret_image,ciphered_color_images[i
]))
        decrypted_images[i].save("images/decrypted_"+RGB_msg[i]+"_"+input_image_name)
    #decrypted_image = generate_decrypted_image(secret_image,ciphered_image)
    combined_image = combine_color(decrypted_images)

    for x in range(combined_image.size[0]):
        for y in range(combined_image.size[1]):
            color = combined_image.getpixel((x,y))
            combined_image.putpixel((x,y),tuple([255-color[0],255-color[1],255-color[2]]))

    combined_image.save("images/Decrypt_"+input_image_name)

if __name__ == '__main__':
    main(argv = sys.argv)
```

Generate_image.py

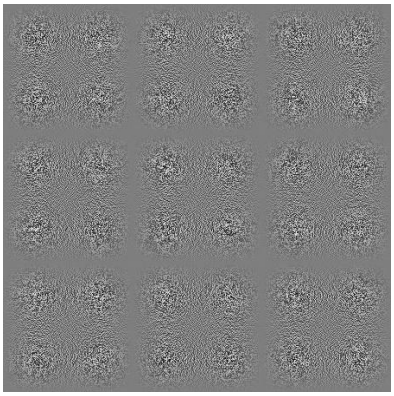
```
import random
from PIL import Image


def separate_color(image):
    w,h = image.size
    color_images = [Image.new(mode="L",size=image.size) for i in range(3)]

    for x in range(w):
        for y in range(h):
            color = image.getpixel((x,y))
            for i in range(3):
                color_images[i].putpixel((x,y),color[i])

    return color_images

def generate_secret(size, secret_image=None):
    width, height = size
    new_secret_image = Image.new(mode="L",size=(width*2,height*2))

    if secret_image:
        old_width,old_height  = secret_image.size
    else:
        old_width,old_height = (-1,-1)


    for x in range(0,2*width,2):
```

```
        for y in range(0,2*height,2):
            if(x < old_width and y < old_height):
                color = secret_image.getpixel((x,y))
            else:
                color = random.randint(0,256)
            new_secret_image.putpixel((x,y),color)
            new_secret_image.putpixel((x+1,y),255-color)
            new_secret_image.putpixel((x,y+1),255-color)
            new_secret_image.putpixel((x+1,y+1),color)

    return new_secret_image



def generate_ciphered_image(secret_image, prepared_image):
    width, height = prepared_image.size
    ciphered_image = Image.new(mode="L",size=(width*2,height*2))

    for x in range(0,2*width,2):
        for y in range(0,2*height,2):
            secret = secret_image.getpixel((x,y))
            message = prepared_image.getpixel((x/2,y/2))
            color = secret ^ message
            ciphered_image.putpixel((x,y),255-color)
            ciphered_image.putpixel((x+1,y),color)
            ciphered_image.putpixel((x,y+1),color)
            ciphered_image.putpixel((x+1,y+1),255-color)

    return ciphered_image


def generate_decrypted_image(infile1,infile2):
    outfile = Image.new('L', infile1.size)
    for x in range(infile1.size[0]):
        for y in range(infile1.size[1]):
            outfile.putpixel((x,y),(infile1.getpixel((x,y))^infile2.getpixel((x,y))))
    return outfile


def combine_color(images):

    image = Image.new(mode="RGB",size=images[0].size)
    w,h = images[0].size
    for x in range(w):
        for y in range(h):
            r = images[0].getpixel((x,y))
            g = images[1].getpixel((x,y))
            b = images[2].getpixel((x,y))
```

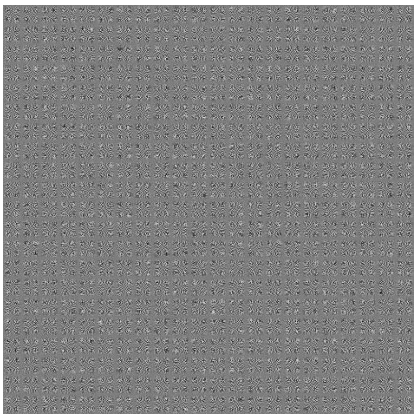
```
            color = tuple([r,g,b])
            image.putpixel((x,y),color)

    return image
```

OUTPUT

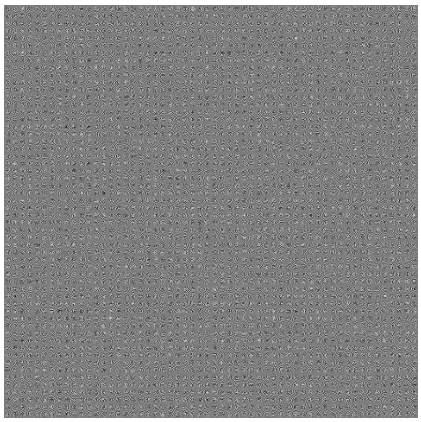
Input_message.png



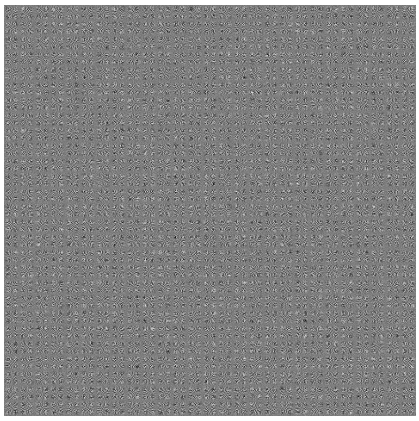
secret_message.png



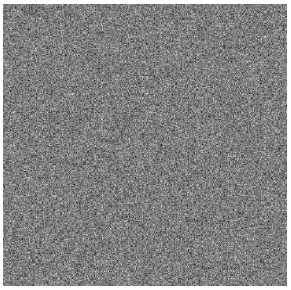
ciphered_R_message.png



ciphered_G_message.png



ciphered_B_message.png



Ciphered_message.png

Decrypted_R_message.png

Decrypted_G_message.png

Decrypted_B_message.png

Decrypted_message.png

CONCLUSION

There are a variety of creative ideas and augmentations of Visual Cryptography proposed since its introduction. The Visual Cryptography strategy is being utilized by various nations for subtly move of manually written archives, budgetary reports, content pictures, web casting a ballot and so forth.

The current visual cryptography plans still lead to pixel extension and inadequate visual quality. Subsequently, further work to upgrade the visual cryptography component for greater security of the data can be done. Coordinating VC plot with computerized watermarking, steganography could be improving the security level of the data.

REFERENCES

- Image Security using Visual Cryptography, Sangeeta Bhuyan, 2012
- An Implementation of Algorithms in Visual Cryptography in Images, ArchanaB.Dhole and Prof. Nitin J. Janwe, 2013
- An extended visual cryptography scheme without pixel expansion for halftoneimages, N. Askari, H.M. Heys, and C.R. Moloney, 2013
- Design and Implementation of a (2, 2) and a (2,3) Visual Cryptographic Scheme,Ujjwal Chakraborty, 2010
- Colored visual cryptography scheme, Verheul & Tilborg, 2015

Plagiarism Report-