A Secure Visual Cryptography For Color Images Using Digital-Watermarking

Prof. S. M. Rokade[1], Ms. Dipali Kunde[2], Ms. Kaveri Phad[3], Ms. Vaishnavi Pathare[4], Ms.Kajal Kapadi[5],

Associate Professor, Computer Department, SVIT, Nashik, Maharashtra, India[1]

Student of BE, Computer Department, SVIT, Nashik, Maharashtra, India[2] Student of BE, Computer Department, SVIT, Nashik, Maharashtra, India[3] Student of BE, Computer Department, SVIT, Nashik, Maharashtra, India[4] Student of BE, Computer Department, SVIT, Nashik, Maharashtra, India[5]

Abstract:

*Visual cryptography is a cryptographic technique which allows visual information (e.g.picture,texts) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme.In visual cryptography encryption of image is done by dividing the image into n number of shares and decryption process is done by combining a certain number of shares or more.simple visual cryptography is not secure because of the decryption process done by visual system.The information or the image can be retrieved by anyone if the person gets at least some number of shares.Secret image can be reconstructed without any complex computation.In this project we use digital watermarking.Digital watermarking is a technique for inserting secret information into an image,which enables us to know the source or owner of the copyrigh*t.

Keywords: Digital-watermarking,Encryption,Decryption,color-image, KN-secret-sharing algorithm,enveloping

Introduction:

Visual cryptography scheme proposed by Naor and Shamir serves as a basic model and has been applied to many applications.Visual cryptography is a cryptographic technique where visual information (for example images,text etc.) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers . Like other multimedia components, image is sensed by human. It is s type of secret sharing scheme by Naor and Shamir. In a k-out-of-n scheme of visual cryptography, a secret image is cryptographically encoded into n shares of random patterns.Pixel is the smallest unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency.

A 32 bit sample pixel is represented in the following figure.

11100111	11011001	11111101	00111110
ALPHA	RED	GREEN	BLUE

Fig 1: Structure of a 32 bit pixel

Human visual system acts as an OR function in visual cryptography. Two transparent objects stacked together, to produce transparent object. But changing any of them to non-transparent, final objects will be seen nontransparent. In k-n secret sharing visual cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the original image. The division is done by Random Number generator . This type of visual cryptography technique is insecure as the reconstruction is done by simple OR operation. To add more security to this scheme we have proposed a technique called digital enveloping or digital watermarking. This is nothing but an extended invisible digital watermarking technique. Using this technique, the divided shares produced by k-n secret sharing visual algorithm are embedded into the envelope images by LSB replacement . The color change of the envelope images are not sensed by human eye .This technique is known as invisible digital watermarking as human eye can not identify the change in the envelope image (Produced after LSB replacement). In the decryption process k number of embedded envelope images are taken and LSB are retrieved from each of them followed by OR operation to generated the original image.

Literature Survey:

1) " Enhancing Security of Image Steganography Using Visual Cryptography "

Author of the paper:- Muhammad Animal Islam ,Md-Al-Amin Khan ,Tanmoy Sorkar Pias

In this paper , text and image are used as a secret message and image for the cover object. 24 bit RGB color image share used as both secret and cover images.

In this method, use a new image namely share1 which converts a secret image to a totally different image called share2 image. Typically, knowing the extraction method, people can retrieve the secret message easily. A pseudorandom ly generated image is used as a key for visual encryption and this ensures the extra layer o f security[1].

2) " Evaluation Criteria for Visual Cryptography Schemes via Neural Networks "

Author: Xiao -nan Lu , Yunchao wang ,Yunfa Li

In this paper, by the aid of neural networks, they propose two criteria called encryption - inconsistency and decryption-consistency for evaluating the shares and the recovered images, respectively. They also implemented the experiments for two representatives of visual cryptography schemes by applying three popular convolutional neural networks

(CNN) to adopt proposed criteria.In this paper we studied that consistency between the shares and original image is very poor.The two schemes implemented in this project is more concerned about quality of shares but are unsatisfactory on recovering the original image[2].

3) "An Extended Visual Cryptography Technique for Medical Image Security "

Author : -Rajitha B, Richa Mauraya ,Ashwani Kumar Kannojiya .

In this paper first encrypts the medical image and then embeds it into 3 cover images. Later on the receiver side, the secret image will be reconstructed from three shares (meaningful) followed by its decryption. The meaningful shares used in the proposed technique uses a block size for each pixel in the secret image. No pixel expansion approach for encryption is proposed in the paper. In this paper we

studied that using steaganography is large overhead to hide very tiny amounts of information,image is distorted and message is easily lost if picture subject to compression such as jpeg[3].

Methodology:

- Encryption process
- K-N secret sharing algortihm
- Enveloping
- Digital watermarking
- Decryption process

System Architecture:(1)

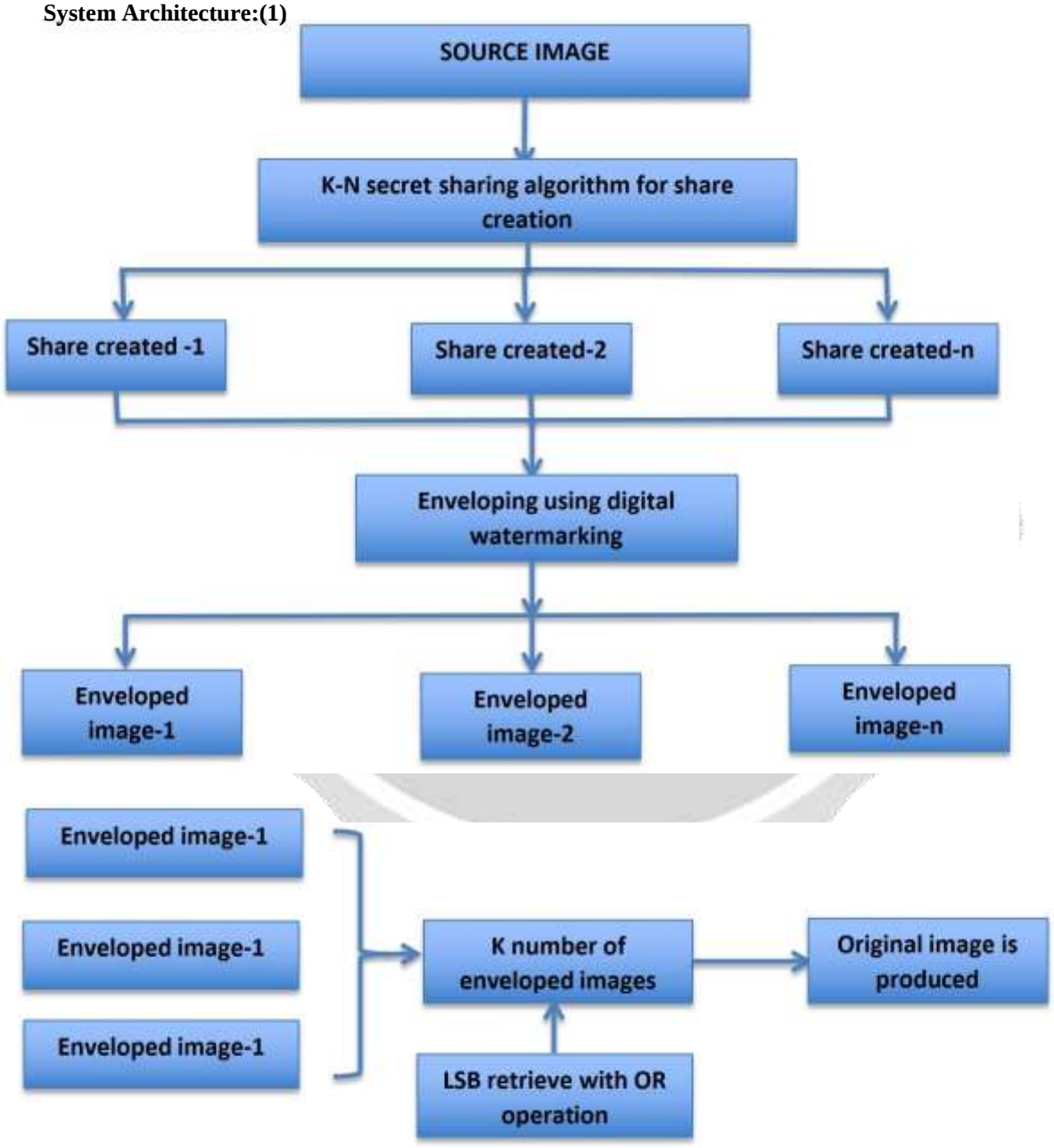

Fig.System Architecture(Encrytion process and decryption process)

Working: In this section we discuss about working methodology of visual cryptography.Visual cryptography can be used to improve the security and privacy of image by embedding digital watermark into it.Actual process of visual cryptography is mentioned below: Any image is divided into number of shares(n) using k-n secret sharing algorithm such that k number of shares are sufficient to reconstruct the original image which is encrypted. the n number of shares generated by using k-n secret sharing algorithm is embedded into n number of different envelope images using LSB replacement algorithm.Again k number of enveloped images generated in step 2 are taken and then their LSB are retrieving with OR operation,then original image is produced .

Techniques used for Encryption and decryption:

K-N secret sharing algorithm:k-n secret sharing scheme is a special type of visual cryptographic technique where at least a group of k shares out of n shares reveals the secre secret information,less of it will reveal no information.In this project we use k-n secret sharing scheme in which image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image.The division is done by random number generator .

Enveloping:Shares of original image are enveloped within other image is called enveloping.LSB that means least significant bit replacement is used for this enveloping process.32 bit digital image pixel is divided into four parts so each part alpha,red,green,blue consist of 8 bits.if the last two bits of each of these parts are changed then the change color is not sensed by human eye.this process is known as invisible digital watermarking..

Decryption process:K numbers of enveloped images are taken as input.from ea ch of these image for each pixel,the last two bits of alpha,red,green,blue are retrieved and OR operation is performed to generate the original image.OR operation can be used for the case of stacking k number of enveloped image out of n.

Result:

Fig -1:Encryption process

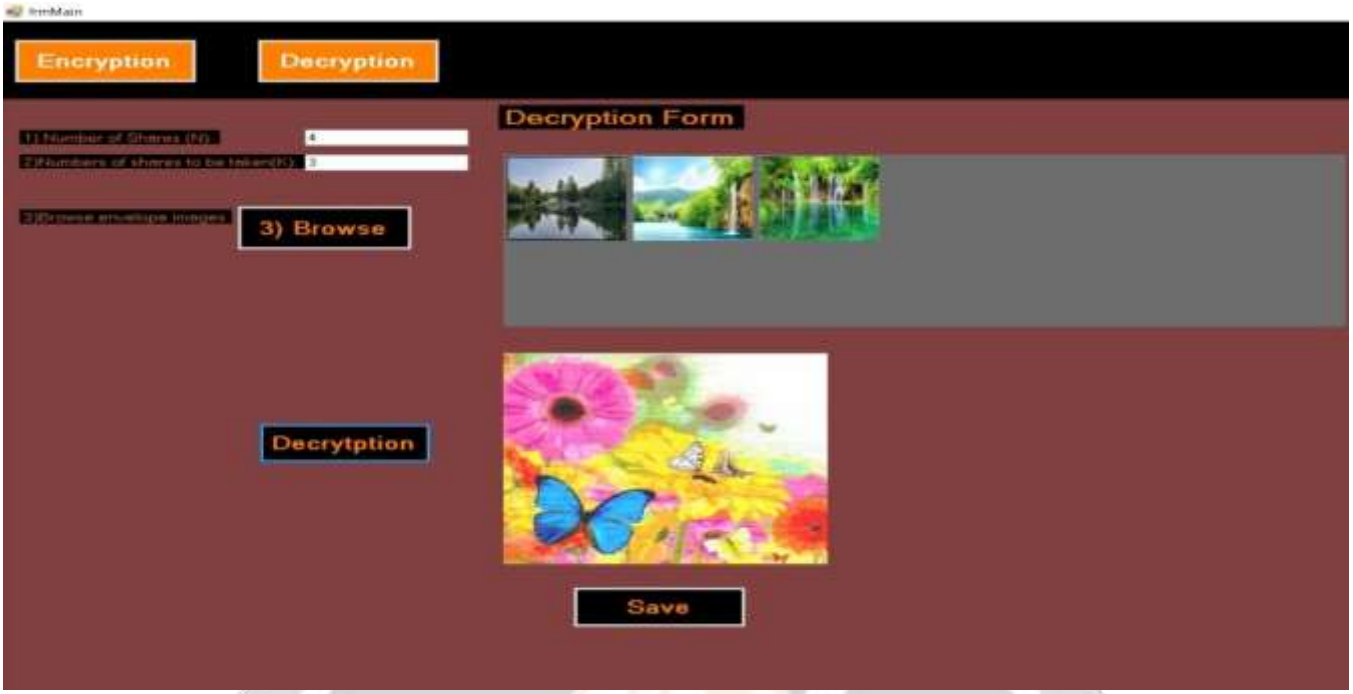

Fig-2 Decryption process

For visual cryptography, we have used different techniques and algorithms. Using that we got the result which is shown in above figure i.e., fig -1 and fig-2.

Conclusion:

In this paper, we used well known k -n secret sharing visual algortihm and enveloping technique Is proposed where the secret shares are enveloped within apparently another digital pictures or covers using LSB replacement with digital watermarking . This additional techniques provide security to visual cryptography technique from illicit attack as it befools the hackers' eye. The division of an image into n number of shares is done by using random number generator, which is a new technique. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers. A comparison is made with the proposed scheme with some other schemes to prove the novelty of the scheme. Decryption part of visual cryptography is based on OR operation, so if a person gets sufficient k number of shares; the image can be easily decrypted

Reference:

1) Muhammad Animal Islam ,Md-Al-Amin Khan ,Tanmoy Sorkar Pias ," Enhancing Security of Image Steganography Using Visual Cryptography" ,2021.
2) Xiao -nan Lu , Yunchao wang ,Yunfa Li," Evaluation Criteria for Visual Cryptography Schemes via Neural Networks" University of Yamanashi,Department of Computer Science and Engineering,Kofu,Japan,400-8510,2021.
3) Rajitha B, Richa Mauraya ,Ashwani Kumar Kannojiya,"An Extended Visual Cryptography Technique for Medical Image Security '',2020.
4) pooja kashyap,A.Renuka,Manipal Institute of Technology Manipal Academy of Higher Education, Manipal, India,"Visual Cryptography for colour images using multilevel thresholding"2020.
5) petre anghelescu,lonela-mariana lonescu,"design and implementation of a visual cryptography",2020
6) V.Annie Daisy,C.Vijesh Joe,S.Shinly Swarna Sugi,Department of IT, Infos ys Pvt. Ltd.,"An image based authentication technique using visual cryptography scheme",2017