Visual Cryptography for Color Image Using Watermarking

Ms.Dipali D Kunde, Ms.Vaishnavi U Pathare, Ms.Kaveri P Phad, Ms.Kajal Y Kapadi, Prof.S.M.Rokade,

Department of Computer Engineering
SVIT Nashik, Maharashtra, India

***Abstract*: Now internet is the fastest growing way of communication. Data exchange over the internet is increasing day by day, so it is important to secure the transmitted in this medium. Visual cryptography technique can be used to improve the security and privacy of the image by embedding watermark .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 copyright.**

***Keywords*: Encryption, decryption, visual cryptography, digital watermarking, color image, K-N secret sharing, enveloping.**

Introduction:
Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without aid of computers [1]. Like other multimedia components, image is sensed by human. 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 [2] [3].

11100111	11011001	11111101	00111110
ALPHA	RED	GREEN	BLUE

Fig 1: Structure of a 32 bit pixel

Human visual system acts as an OR function. Two transparent objects stacked together, 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 image. The division is done by Random Number generator [4]. 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. This is nothing but an extended invisible digital watermarking technique. Using this technique, the divided shares produced by k-n secret sharing visual cryptography are embedded into the envelope images by LSB replacement [5]. The color change of the envelope images are not sensed by human eye [6]. (More than 16.7 million i.e.224 different colors are produced by RGB color model. But human eye can discriminate only a few of them.). This technique is known as invisible digital watermarking as human eye cannot identify the change in the envelope image and the enveloped (Produced after LSB replacement) image [7]. 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. In this project describes the Overall process of Operation, Section 3 describes the process of k-n secret sharing Visual Cryptography scheme on the image, Section 4 describes the enveloping process using invisible digital watermarking, Section 5 describes decryption process, Section 6 describes the experimental result, and Section 7 draws the conclusion.

Problem Statement – Visual Cryptography technique can be used to improve the security and privacy of copyright protection of image by embedding watermark so to share the secret image without reveling the original image and third party cannot decrypt the image if he has less than the required number of shares using visual cryptography. So to secure the image sharing over the internet we proposed visual cryptography using digital watermarking.

Objective –The objective of visual cryptography is to make image incomprehensible unauthorized person
2) Cryptography protects the confidentiality of information even when the transmission or storage medium has been comprised the encrypted information is practically useless to unauthorized person without having the proper knowledge of decryption

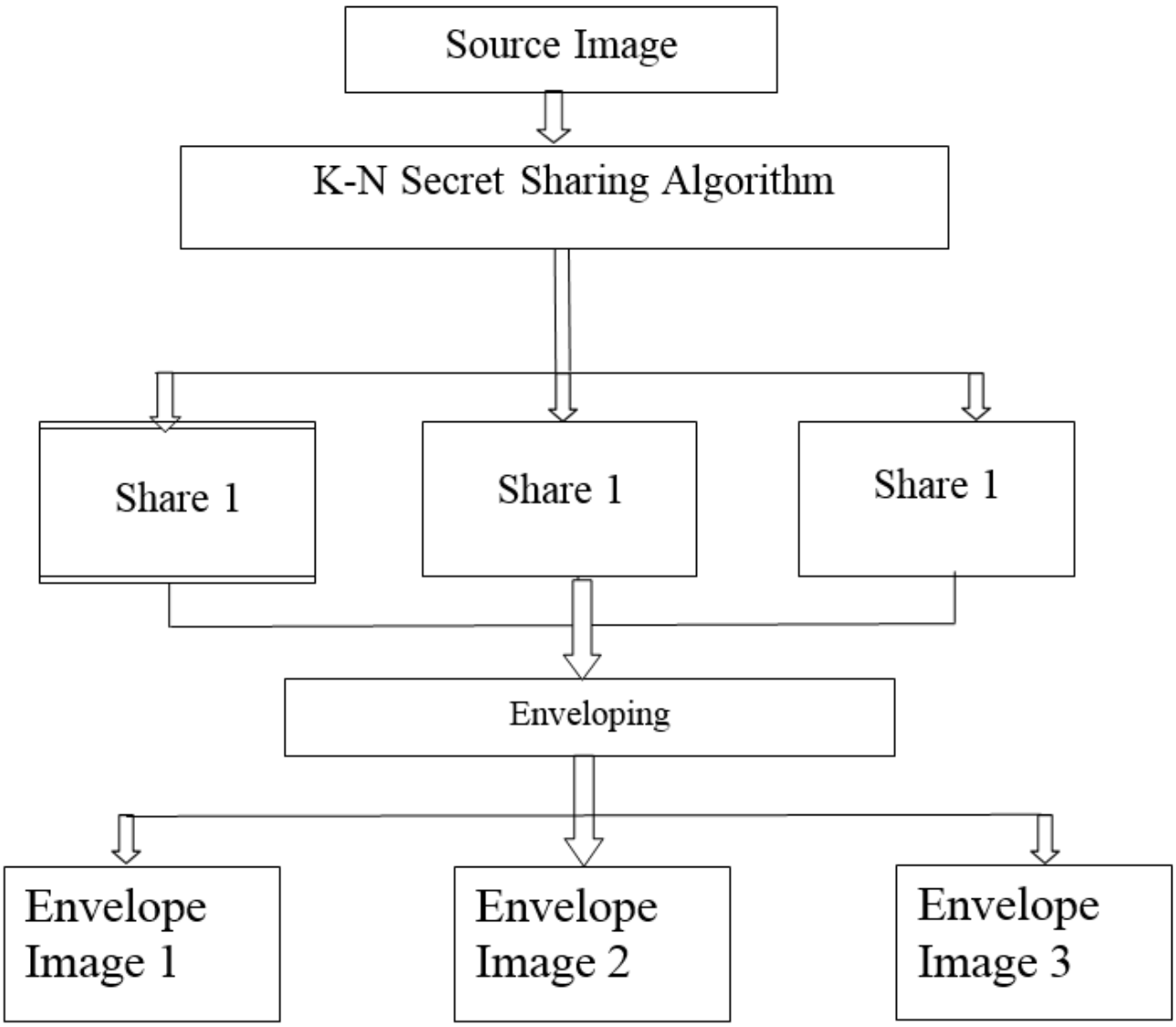
Literature Survey –
"Evaluation Criteria for Visual Cryptography Schemes via Neural Networks"Author: Yunchao wang Yunfa Li Xiao -nan Lu
In this paper, by the aid of neural networks, they propose two criteria called encryption - inconsistency and decryption-consistency

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.

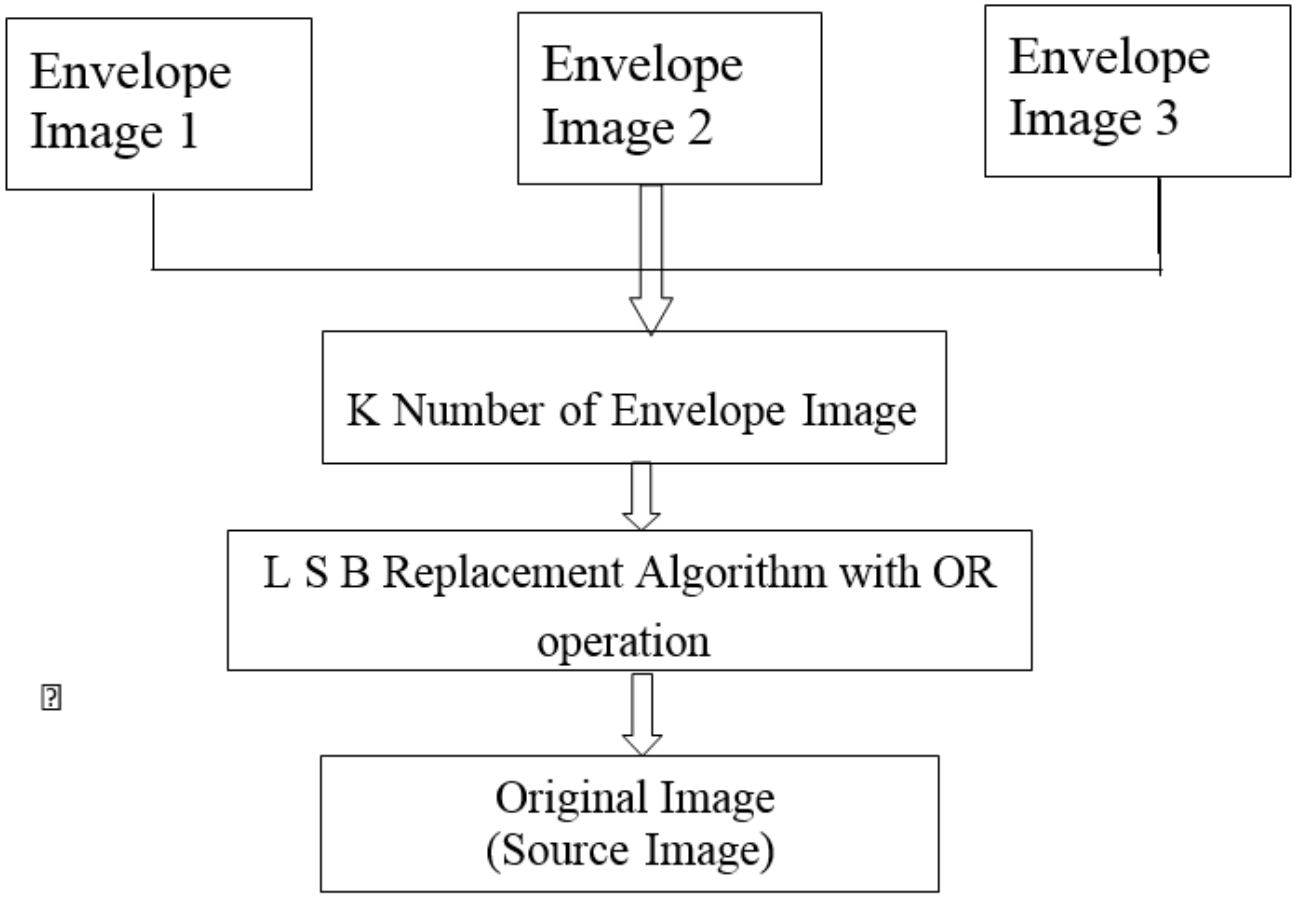
"An Extended Visual Cryptography Technique for Medical Image Security " Author : - Richa Mauraya, Ashwani Kumar, Kannojiya Rajitha B.
In this paper first encrypts the medical image and then embeds it into 3 cover images. Later on the receiver side, the secret image will be reconstructed from three shares (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 steganography 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.

"Enhancing Security of Image Steganography Using Visual Cryptography " Author :- Muhammad Animal Islam, Md-Al-Amin Khan Tanmoy Sorkar Pias
In this paper method, 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 of security.

System architecture:
This section present the listing of proposed system architecture for a visual cryptography technique.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:
1) 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.
2) 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.
3) 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.
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 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 each 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.



ENCRYPTION PROCESS



DECRYPTION PROCESS

Algorithm:

1) K-n secret sharing algorithm: This algorithm is proposed to divide the image into n number of shares. An image is taken as input. The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The division is done by following steps: 1)Take an image as input and calculate its width and height 2)Take the number of shares and minimum number of shares to be taken to reconstruct the image where k must be less than or equal to calculate recons=(n-k)+1. 3)Create a three dimensional array to store the pixels of n number of shares .scan each pixel value of image and convert it into 32bit binary string. 4)create a one dimensional array to store constructed pixels of each n number of Shares. Construct alpha, red, green, and blue part of each pixel by taking consecutive 8 bits substring starting from 0.Construct pixel from these part and store it into array.

2) Enveloping using Digital Watermarking In this step the divided shares of the original image are enveloped within other image. 1) Take number of shares as input 2) Take the name of the share and name of envelope as input. Let the width and height of each share w and h. The width of the envelope must be 4 times than that of share no. 3) Create an array of size w*h*32 to store the binary pixel values of the share no using loop. 4)Embed share no within envelope no.construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0.Construct pixel from these part and store it into a one dimensional array and generate image.

Advantages –

1. Authentication: The cryptography technique such as digital watermarking can protect information against forgenes.
2. Confidentiality: Encryption technique can guard the information communication from unauthorized revelation and process of information.
3. Non-Repudiation: The digital signature provides the non-repudiation service may arise due to devial of passing message by the sender.

Disadvantages:

1. Strongly encrypted, authentic and digitally signed information can be difficult to access.
2. 2. Selective access control.

Application:

1. Military purpose: It's a way military can securely transmit location using map picture or any information.
2. Examination System: It can also useful for transferring question paper so no one can decrypt that.
3. Medical images: Healthcare provides generate large amounts of medical imaging data so these digital records need to be processed and stored securely for that purpose we can use visual cryptography.

Conclusion –

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. In this current work, with well-known k-n secret sharing visual cryptography scheme an enveloping technique is proposed where the secret shares are enveloped within apparently innocent covers of digital pictures using LSB replacement digital watermarking. This adds 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 not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images [10][11][12][13]. 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.

References–

[1] petre anghelescu,lonela-mariana lonescu,"design and implementation of a visual cryptography",2020
[2] Rajat Bhatnagar,Manoj Kumar,"Visual cryptography",march-2018
[3] Annie daisy,vijesh joe,shinly swarna sugi,"An image based authentication technique using visual cryptography",october-2017.
[4] richa maurya,ashwani kumar kannojiya,b rajitha," an extented visual cryptography technique for medical image security" Motilal Nehru National Institute of Technology Allahabad, Prayagraj, India,2020.
[5] pooja kashyap,A.Renuka,Manipal Institute of Technology Manipal Academy of Higher Education, Manipal, India,"Visual Cryptography for colour images using multilevel thresholding"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