K-n Share Generation for Securing Color Images Using Visual Cryptography

Robin Renji Abraham[1], Jeena P Achenkunju[2], Aneena Thomas[3], Gouri R Sekhar[4], Rincy Roy Oommen[5]
[1234] *Student,Department of Computer Science & Engineering, Mount Zion College of Engineering, Kerala, India*
[5]*Assistant Professor, Department of Computer Science and Engineering, Mount Zion College of Engineering, Kerala, India*

***Abstract*- Cryptography is a way through which information can be made invisible to the users by encrypting them. The visual cryptography permits user outlined pictures to be divided into multiple range of shares known as clear shares (Transparent Shares). A color image to be protected and a binary image used as key to write and re-write square measure taken as input. After applying the visual cryptographic technique, then solely the pictures square measures to be transmitted; As a result the hacker cannot perceive the distorted image and thus the digital communication become secured. The most notable feature of this approach that it will recover a secret image with none computation. It exploits the human sensory system to browse the key image from few overlapping shares. Thus overcomes the disadvantage of advanced computation needed within the ancient visual cryptography. Mainly this paper describes however color image cryptography and decipherment tired visual cryptography by generating multiple shares. Blowfish algorithmic rule is used for color image cryptography and decipherment in visual cryptography. The planned technique is additionally enforced in Matlab for RGB color pictures.**

Index Terms- Visual Cryptography, VCS, EVCS, Blowfish, RGB color image, Share Generation, Encryption.

I. INTRODUCTION

In recent days, network security has become a main issue. Cryptography has come back up as an answer and place a crucial role in network security system. Several strategies area unit required to protect the shared knowledge. Owing to the growing demand for info security, image cryptography and decoding has become a major analysis space and it's broad application prospects.

A. Cryptography

Cryptography may be a means through that info is created invisible to the users by encrypting them. It's the study and implementation techniques to cover information or just to guard a message or text from being browse.

B. Visual Cryptography

Visual Cryptography may be a secret sharing theme for encrypting a secret image, it is a superbly secure means that enables secret sharing with none science computation that is termed as Visual Cryptography Scheme (VCS). This enables digital pictures is split into shares referred to as clear shares and every share holds some info. Once all shares combined along, they have a tendency to show the key of the image .it is unable to reveal any knowledge on the first image if at least one among the shares isn't achieved. The first image, in fact is completed by overlapping the whole shares directly, in order that the human sensory system is competent to spot the collective secret image while not using any difficult machine tools.

II. RELATED WORKS

M Karolin, Dr. T. Meyyappan, SM Thamaraai [1], proposed a visual cryptographic technique that can be used to generate only 2 shares of the secret image .Here the secret color image can be converted to black and white binary image. Blowfish algorithm is used for encoding and decoding of datas. This technique can be used for secure data transmission. Steganography can be also introduced along with this cryptographic technique for both encryption and decryption of color images.

M Karolin [2], proposed a method for images with the 256 colors which are converted to 16 standard

RGB colors format. It generates shares without compromise the resolution. The Floyd Steinberg Dithering algorithm is used to manipulate the 256 color code image to decrease it to 16 standard color code image. The proposed method employs (2, 2) X-OR based visual cryptography method is used to generate shares. Decryption procedure enables secret image sharing and stacking. The proposed method converts the 256 color image to 16 color code format for the share formation, the intensity of the original image is maintained.

Jayadeep Veena, Vineeth Khemchandani [5], introduced visual cryptography encryption. It consist of generation of shares using any basic visual cryptography model. In this, a (2, 2) VC share creation is performed. Each pixel in the secret image is broken into 4 sub pixels. A white pixel is shared into 2 identical blocks of 4 sub pixels. A black pixel is shared into 2 complementary blocks of 4 sub pixels. All the pixels in the secret image are encrypted similarly using this scheme (visual cryptography encryption).

Feng Liu, Chaurakun Wu [7], introduced a Visual Cryptography Scheme (VCS) which may be a reasonably secret sharing theme that focuses on sharing secret pictures. It allows us to split a secret image into 2 random shares which separately reveals no information about the secret image other than the size of the secret image. EVCS is a kind of VCS which consist of meaningful shares. Construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it as embedded EVCS.

Feng Liu, Wei Qi Yan [8], studied that VCS is for image encryption and decryption without complicate computation, the decryption is performed using human vision system that is the operation is fast, no information exchanges and communication between VCS shares. It is a secret sharing system. The key image consists of black and white pixels. The original secret image is recovered by superimposing 2 shares together. The underlying operation of such a scheme is the logic operation OR. Generally a (k, n), VCS takes a secret image as input and outputs ‘n’ shares that satisfies two conditions.

i. Any k out of n share images can recover secret image.

ii. Any less than k share images cannot get any information about the secret image.

III. EXISTING SYSTEM

Visual Cryptography could be a kind of cryptography within which pictures is firmly encrypted by dividing them in an exceedingly distorted image referred to as clear shares and transmitted physically by printing these shares on transparency sheets to the meant users. Visual cryptography assumes several forms like for grayscale pictures, black and white pictures yet as color pictures. The essential model of visual cryptography for color pictures consists of 3 phases. The primary section to understand color visual cryptography theme is to print the color within the secret image on the shares directly. It performs larger constituent expansions that scale back the standard of the divided color image. The second phases converts a color image into black and white image on the 3 color channels (Red, Green, Blue or equivalently cyan, magenta, yellow) severally, then applies the black and white visual cryptography theme to every of the color channels. This ends up in decrease of constituent enlargement of additional variety of pixels however reduces the standard of the image thanks to halftone method. The third phases utilize the binary illustration of the color of a constituent and encodes the encrypted secret image at the bit-level. This ends up in higher quality however needs devices for decipherment method. Within the RGB model (Red, Green, and Blue), color pictures square measure thought of. Floyd Steinberg video digitizing formula is employed to remodel the 256 code pictures to low code image. It achieves the video digitizing exploitation error diffusion and takes the closest neighbor constituent to form the share. The RGB code is separated into sixteen normal code formats while not reduction within the resolution. The video digitizing formula is employed rather than halftoning. Separate array is formed to every share and manipulated. This analysis work extends to ensuing level to secure the key image through secret writing and secret writing exploitation Blowfish formula. Matlab tool is utilized for implementing the planned methodology.

Blowfish Bruce Schneier designed blowfish in 1993 as a quick, free totally different to existing cryptography algorithms. Since then it's been analyze significantly, and it's slowly quick acceptance as a powerful cryptography algorithmic rule. The Blowfish algorithmic rule has several blessings. It's

appropriate and economical for hardware implementation and no authorize is needed. The essential operators of blowfish algorithmic rule embody table operation, addition, and XOR. Blowfish may be a cipher supported Feistel rounds, and also the setup of the F-function used amounts to a generalization of the principles employed in DES to produce constant security with larger speed and potency in software package. Blowfish may be a 64-bit block cipher and is ex gratia as a alternate for DES. Blowfish may be a quick and free algorithmic rule and might encode knowledge on 32bit microprocessors. Therefore during this paper, we have a tendency to are implementing blowfish algorithmic rule that is strongest and quickest in processing store measure to alternative algorithms. Blowfish algorithmic rule is basically secured as a result of it's longer key length thirty two to 448 bit (more no of key size).

IV. PROPOSED SYSTEM

Visual cryptography includes breaking up the image into n shares in order that solely somebody with all n shares could decrypt the image by overlaying each of the shares over each other. In the proposed system total of n shares of the image is generated according to the user need and from these shares k number of shares are selected to get the secret image. The multiple shares are generated by applying Floyd-Steinberg algorithm and these shares are encoded using Blowfish algorithm.

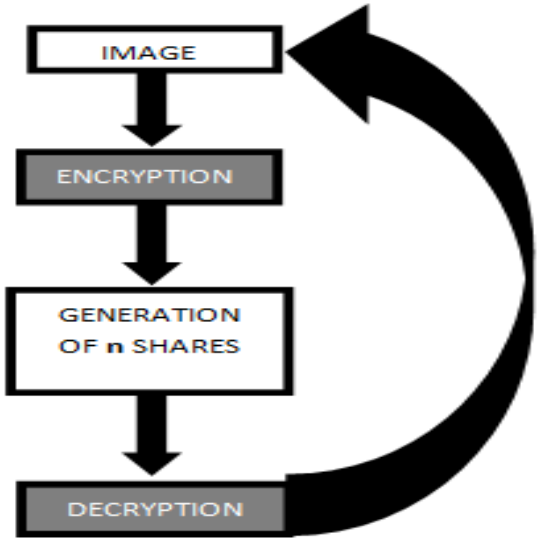

Fig:1. System Model

A. Steps for share generation processor

- Contemplate the input secret image because the RGB model color image.
- The input image is currently fed to the error diffusion method that uses Floyd – Steinberg rule to diffuse the image.
- Repeat Step-2 till each picture element within the image is rotten. The video digitizing method then computes the quality sixteen named color codes.
- This step ends up in generation of n shares (transparencies) of the key image.
- Finally, the stacked image is created by combining the at least k shares that square measure generated.

B. Steps within the rule

- Input the input secret image in the RGB model color image.
- Input the value of k and n.
- Produce the key price having thirty two to 448 bits.
- Applying Blowfish rule for encryption.
- Decipher the encrypted image by using identical key.
- End.

C. Encoding method

Original image and encoding key square measure input to the encoding method. The bit stream of the first image is separated into blocks length of Blowfish rule.

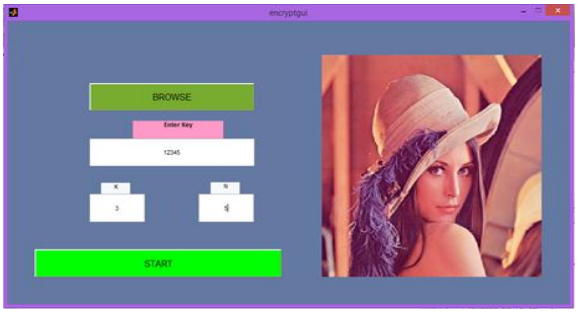

Fig:2. Input for encryption

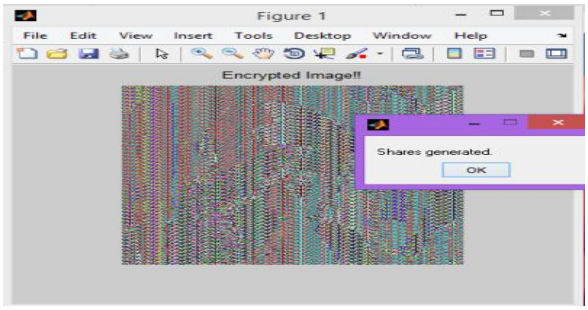

Fig:3. Encrypted image

D. Coding method

The encrypted image is split into identical block length of blowfish rule from prime to bottom. The blocks square measure subjected to secret writing operate. Identical encoding secret is accustomed decipher the image by reversing the operate of sub keys is reversed. To decipher the encrypted image, select k number of shares that have been generated during encryption process and enter the identical key and obtain the secret image.

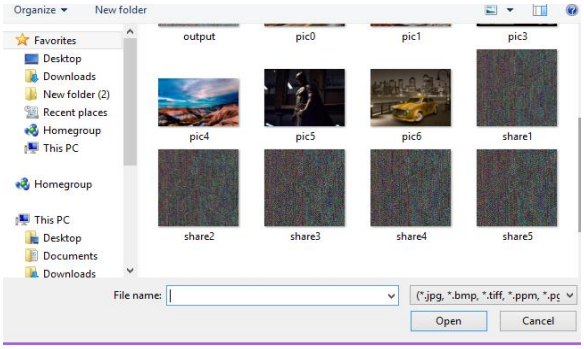

Fig:4. Shares Generated

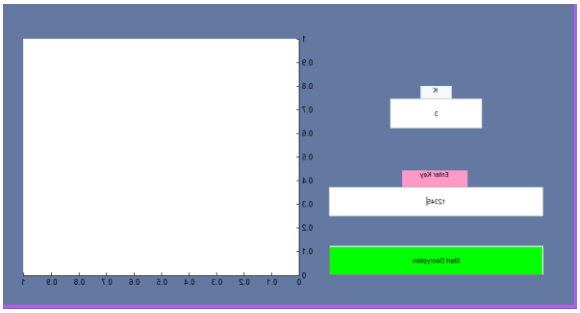

Fig:5. Decrypting the image

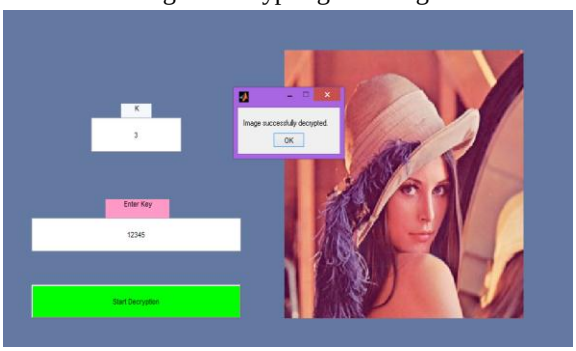

Fig:6. Decrypted image

V. RESULT AND DISCUSSION

The proposed model encompasses share generation, encryption and decryption of the secret image. The share generation process creates n shares of the image and encrypted using blowfish algorithm. The distorted image can be decrypted by selecting k number of shares from a total of n shares. Thus we retrieve the original image. This provides authentication, authorization and confidentiality for message passing. Thus restrict access to any third parties who try to steal the data and information.

VI. CONCLUSION

The visual cryptography procedures transmits computerized picture safely. The method isolates the mystery picture into different printable offers which misuses the human vision framework. That is Original picture which contains mystery data is misshaped. With the goal that the programmer can't comprehend the twisted picture and transmit the picture safely. The blowfish calculation encodes information on 32-bit chip at the rate of 26 clock cycles for each byte. It keeps running in under 5k of memory. It has variable key length. Key length fluctuates from 32-448 bits. Default key length is 128 bits.

Blowfish is a keyed that decides the useful yield of cryptographic calculation, symmetric cryptographic square figure. It has been dissected significantly and it is gradually picking up acknowledgment as a solid encryption calculation. Blowfish is reasonable for application where the key doesn't change often, similar to a correspondence connect or a programmed document encryption. It is essentially quicker than most encryption calculation, when on 32 bit microchip with extensive information reserves. In this strategy mystery picture is partitioned into various straightforward offers which misuses the human vision framework. This conquers the computational unpredictability of conventional cryptography.

Blowfish calculation is utilized for shading picture encryption and unscrambling in visual cryptography for verifying the picture. The proposed system is actualized with matlab coding. Blowfish has a superior exhibition than other basic encryption calculation utilized since blowfish has no known security frail focuses. So far which makes it a great possibility to be considered as a standard encryption calculation.

ACKNOWLEDGEMENT

The authors would like to thank everyone who supported to do this study and also thank to Mount Zion College of Engineering for giving a platform to do this work

REFERENCES

[1] M.Karolin, Dr.T. Meyyappan,SM.Tamarai ,"Encryption and Decryption of Color Images using Visual Cryptography."(2018)
[2] M.karolin Dr.T.Meyyappan,"RGB Based Secret Sharing Scheme in Color visual cryptography",in International Journal (2015)
[3] Shankar, and P.Eswaran. "RGB based different offer creation in visual cryptography with help of elliptic bend cryptography."(2017)
[4] J.Tamilarasi, V. Vanitha, T. Renuka,"Improving Image Quality In Extending Visual Cryptography for Halftone Images with No Pixel Expansion", in International Journal of Scientific and Technology Reasearch(2014)
[5] Jagdeep varma, Dr.Vineeta Khemchandani,"A visual cryptographic method to verify Image shares(2012)
[6] Tingyuan Nie., Teng Zhang," An investigation of DES and Blowfish Encryption Algorithm", IEEE (2009)
[7] Feng Liu,Wie Qi Yan,"Visual Cryptography for Image Processing and security."
[8] Tingyuan Nie,Teng Zhang,, "A study of DES and Blowfish encryption algorithm".