ENHANCED VISUAL CRYPTOGRAPHY TECHNIQUES

P.N.SAI NATH SHARMA[1], Mr. PRAVEEN CHOUSKEY[2]

[1]M. TECH (CSE) Scholar Department of CSE Dr. C.V. Raman University Bilaspur

[2]Associate Prof. Department of CSE Dr. C.V. Raman University Bilaspur

Abstract

Visual Cryptography is one of the reliable technique for the security purpose. In this technique we divide the image into shares and then these shares are encrypted using encryption algorithms. Visual Cryptography is done on black and white image as well as on color image. This paper includes the literature survey regarding Visual Cryptography techniques.

Keywords: Cryptography, Data Encryption Standard (DES), Keyed Visual Cryptographic Scheme (KVCS), Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD).

Introduction

In recent days network security has become a main issue. Encryption has come up as a solution, and plays an important role in network security system. Many methods are needed to guard the shared data. Because of the growing demand for information security, image encryption decryption has become a significant research area and it has broad application prospects.

1.1 Cryptography

Cryptography is a way through which information can be made invisible to the users by encrypting them. It is the study and implementation of techniques to hide information, or simply to protect a message or text from being read.

1.2 Visual Cryptography

Visual cryptography is a powerful 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. Visual Cryptography Schemes (VCS) is a technique of image encryption novel to hide the secret information in images. Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography. It uses two or more transient images (called shares).One picture contains arbitrary pixels and the other picture contains the secret information that is hidden. It is not possible to recover the secret information from any one of the pictures (images). Either transparent images or layers are required to reveal the secret information. The simple method 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 one-time pad system and will offer unbreakable encryption. In the overlay animation it can be observed by sliding the two layers over layers are required to reveal the secret information. The simple method 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 one-time pad system and will offer unbreakable encryption. In the overlay animation it can be observed by sliding the two layers over layers are required to reveal the secret information. The simple method 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 one-time pad system and will offer unbreakable encryption. In the overlay animation it can be observed by sliding the two layers over layers over

Literature review:

According to [1] Er. RimsyDua et al (2016) In this paper they have effectively implemented the proposed methodology using DES (Data Encryption Standard) algorithm. This concept is enhanced by the transformation of meaningless to meaningful shares and the security is enhanced by using DES algorithm with the help of which shares of secret image are encrypted. The tool that they have used for the implementation of proposed scheme is MATLAB

According to [2] Vinita Malik et al (2016) In this paper they propose a new algorithm for colored visual cryptography and making it more safe with the help of Digital Enveloping technique by applying it on the shares of the image. Digital Enveloping is method in which shares of the image to be sent are distributed over a variety of sample images to generate the enveloped images. At the receiver end, shares are retrieved from the enveloped images and combined to form original image without corrupting the quality of image. Decryption procedure of visual cryptography is based on OR operation, so if any person get all the shares; then the image can be easily decrypted by him. They introduced ARGB Algorithm for secret sharing of colored images along with the enveloping scheme that was previously proposed in which ARGB shares are enveloped within the covers of images using LSB replacement. Hence, this technique increases the security of visual cryptography technique from the attack of hacker as he is not able to retrieve the images without having all the 4 enveloped images.

According to [3] Ch. Rupaet al (2016) In this paper they proposed a new proposal that is Keyed Visual Cryptographic Scheme (KVCS) to reduce the attack by hacker. KVCS is used to raise the computation factors which provide more security to data of image. In KVCS, every input share of original image is encrypted with a shared key share using mathematical operators. At the end, the original image which should be shared secretly would be encoded into two shares and sent

According to [4] Miss. Kashmira S. Gulhaneet al (2016) In this paper the Image is divided into parts known as shares and then these shares are distributed to the participants. In Decryption phase stacking the share images gets the original image. For the RGB/CMY Images different methods are developed which are based on the color decomposition techniques. The Decryption process is very easy generated shares are printed on transparencies. Transparencies are overlapped on top of the other gets the secret image. The displacement of pixels and rearranging of the image in steps between the processes has proven to be valuable. The extra transposition of RGB values in the image file after RGB component reshape has proven to increase the security of the image against all probable attacks available currently

According to [5] Kalyan Daset al (2016) In this paper they have applied Sliding Puzzle Technique on the images and showed good result without any alteration. The algorithm proposed by this scheme reduces the time for encryption and decryption of images in a much easier way and it ensures the lossless transmission of images. Encryption is carried out on the basis of RGB values of pixels. Hybrid approach to visual cryptography where they take colored images and split the image into multiple rows and columns,

resulting image tiles. For decryption, they have (row*col)! Combinations out of which only one gives back the original image. For this purpose symmetric key is used.

According to [6] NidhalKhdhair El Abbadiet al (2016) In this paper they suggested a new method of image encryption based on three major steps: the first step aims to scrambling the image values with Fibonacci transform. The second step aims on generating public and private key based on Diffie-Hellman key exchange, these keys used to encrypt the diagonal matrix which are formed by (SVD) Singular Value Decomposition .In third step, decryption is the contrary to encryption. The results were assured and the decrypted image is retrieved without any loss in its information.

According to [7] K.Kanagalakshmet al (2016) In this paper they proposed a method that is based on Blowfish algorithm with superior features. It has been enhanced with the help of a supplementary key approach to strengthen the security of image or any sensitive data which are communicated by electronic means. The proposed algorithm is developed and tested with different sets of data. The performance of the proposed methods is considered in terms of time, space complexity and security also. The results are recorded and a better performance is observed.

According to [8] Gaurav Kumar et al (2016) In this paper they have purposed a new technique known as digital watermarking as the simple visual cryptography is not so secure for sharing of data and it also does not ensure the user authentication. In this cryptographic technique secret images are divided into n shares and a certain number of shares (m) are sent over the network. This project presents an approach in which visual cryptographically generated image shares are embedded in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images. The shares are embedded into the host image in Frequency Domain using Discrete Cosine Transform (DCT).The weakness of binary secret shares is overcome by hiding them invisibly into the host images. In decryption phase, the secret shares are extracted from their cover images without need of any cover image characteristics because the watermark extraction scheme is blind. The overlapping of these shares reveals the original secret image. The decoded secret image quality is enhanced.

According to [9] Asha BhadranR (2015) In this paper presents a visual cryptography technique for color images in which the generated shares are again encrypted. For this XOR operation is used and this will provide double security for the secret document. Secret shares are not available in their actual form for any modification by the adversaries who try to create fake shares. The proposed method uses the concept of half toning. When the color image is given as input, decoded image was color halftone image.

According to [10] M.Karolinet al (2015) In this paper they proposed a method for images with 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 colors code image. The proposed method employs (2, 2) XOR-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.

According to [11] Manika Sharmaet al (2013) In this paper they proposed a cryptographic technique for color images where we are using color error diffusion with XOR operation. To add more security to the secret sharing of the image Invisible Digital Watermarking is used which protects the secret image from the hacker. Random number procedure is used to generate the shares. In decryption process use

RSA algorithm. This approach produce a reduced amount of unclear image and the size of the decrypted image is equivalent as the original image

According to [12] Sozan Abdulla(2010) presents a system which takes four pictures as an input and generates three images which are in contact with three of the four input images. During the process of decoding, they just select a small number of subset from all of the three images, in order to make the transparencies of them. They stacked them in Last In First Out manner. In this method, after splitting the original image to a number of shares and applying the recoloring procedure. According to the color combination groups they predict the adversary may find out some useful information such as the shape or pattern of the original secret image. Reconstructed image which is obtained is of same size as that of original secret image

Methodology:-

There are two forms in which the Enhanced Visual Cryptography can be implemented. They are Encryption Methodology and Decryption Methodology.
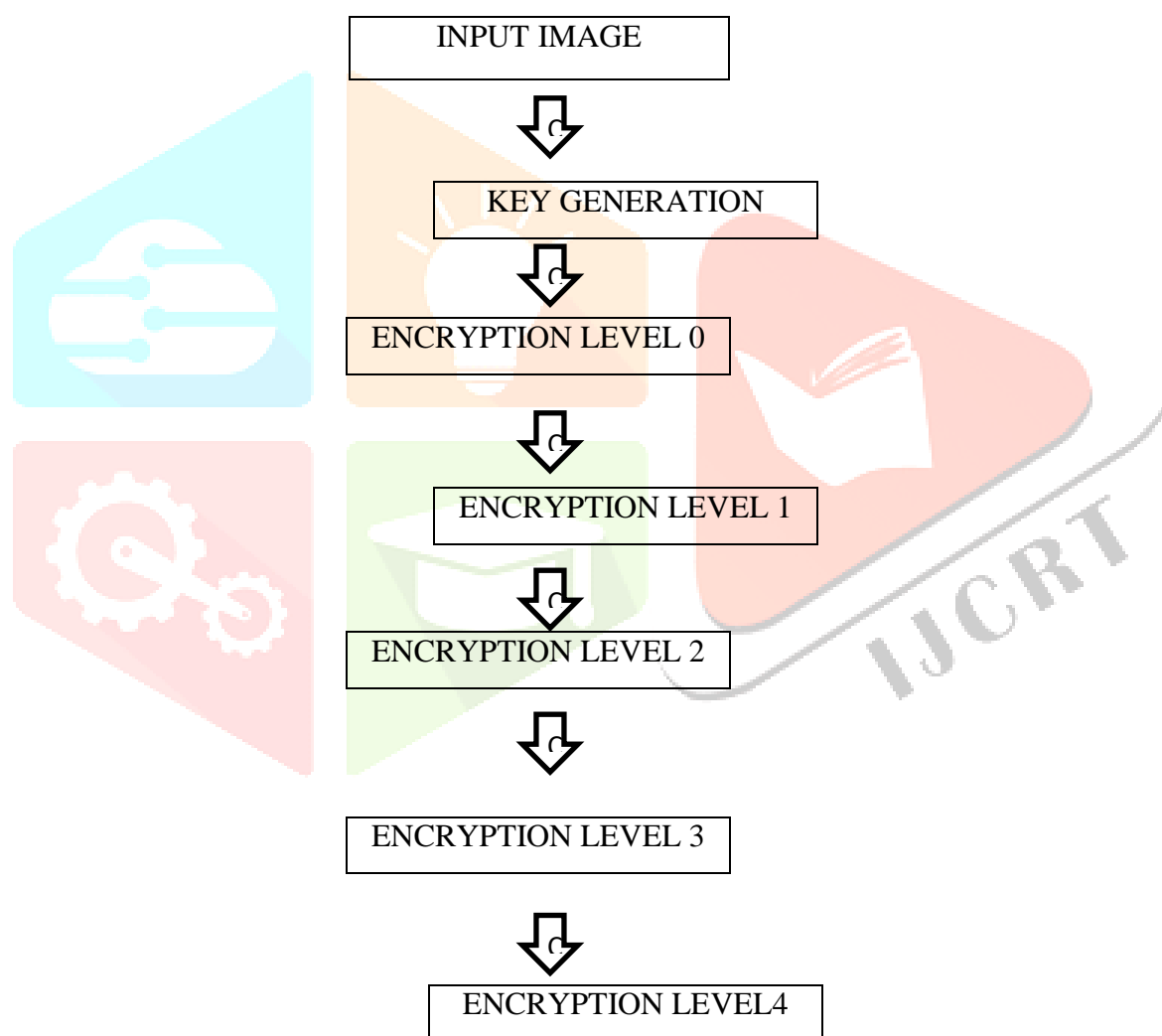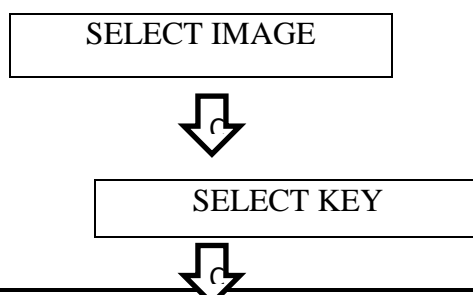

INPUT IMAGE

⬇

KEY GENERATION

⬇

ENCRYPTION LEVEL 0

⬇

ENCRYPTION LEVEL 1

⬇

ENCRYPTION LEVEL 2

⬇

ENCRYPTION LEVEL 3

⬇

ENCRYPTION LEVEL4

FIG.ENCRYPTION METHODOLOGY

SELECT IMAGE

⬇

SELECT KEY

⬇

DENCRYPTION LEVEL 4

⇩

DENCRYPTION LEVEL 3

⇩

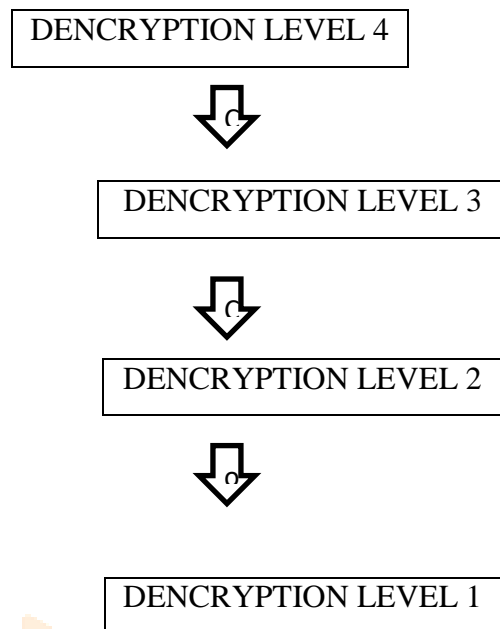DENCRYPTION LEVEL 2

⇩

DENCRYPTION LEVEL 1

FIG.DENCRYPTION METHODOLOGY

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient. **Decryption** is the process of transforming encrypted information so that it is intelligible again.

In Encryption methodology first the required image is imported as input. And a suitable key is generated for the particular imported image. And there are four levels of encryption they are level 0, level1, level 2, level 3 and level 4 encryption. As increasing the level of encryption the more and more the security of the image will be increased.

And Decryption methodology the required image is selected and then the decryption key will be used and decryption level we be initiated by level 4, then level 3 and level 2 then level 1 and last level 0. This means in reverse sequence the decryption will be done because the levels were increased initially for the encryption and in decryption case the it will be in descending order.

Conclusion and future work :-

In order to protect confidential data, we need some security measures. Visual Cryptography provides an effective and efficient way for providing security to a digital image. Using Visual Cryptography, the quality of an image can also be improved. This review paper contains information regarding the techniques that are used to provide security to a digital image. The future scope of the work is to use 3D Images instead of 2D for creating shares and also improve the contrast of decoded secret image.

References:-

[1] Er. RimsyDua, Er. Narender Singh,"Enhancement of security in Visual Cryptography using DES algorithm" in IJIRCCE , July-2016, Vol. 4, Issue No.7.
[2] Vinita Malik,MamtaGhalan,Dheerajkaushik, "Securing of colour images using Visual Cryptography and Digital Enveloping", in COMPUSOFT IJACT, April-2016, Vol. 5, Issue No.3.
[3] Gauravkumar,Sachinchaudhary, "A Visual Cryptography scheme to secure black and white image shares using Digital Watermarking " in IJARCSSE, Volume 6 Issue 5, May 2016.
[4] KalyanDas,Aromitasen,SamirkumarBandyopadhyay,"A new Visual Cryptography scheme for color images using sliding puzzle technique" in IJIRR, Volume 03, Issue 04,April 2016.

[5]]Er. RimsyDua,Er. Narender Singh, "Secured Visual Cryptography scheme using meaningful shares" in IJIRCCE, Volume 4, Issue 4,April 2016.

[6] Ch. Rupa, D. Sasidhar, "Keyed Visual Cryptography scheme for secure data transmission" in 2016.

[7] K.Kanagalakshm, M.Mekala, "Enhanced Blowfish algorithm for image encryption and decryption with supplementary key "in IJCA, Vol. 146-No 5,July 2016.

[8] NidhalKhdhair El Abbadi,SamerThaabanAbbas,AliAbdAlaziz, "New image encryption algorithm based on Diffie – Hellman and Singular value Decomposition " in IJARCCE, Vol. 5, Issue 1, January 2016.

[9] Monika Bhosale, RajshreeChaudhary, PrathameshGaddam, AyushiKedarYogesh. J.Pawar, "Visual Cryptography Scheme for Secret Image Retrieval", Vol. 3,Issue 3 March 2016.

[10] Miss. Kashmira S. Gulhane,Prof. P.L.Ramteke,"VISUAL CRYPTOGRAPHY USING IMAGE"in IJRISE, Vol. 2, Issue 1,2016.

[11] AshaBhadranR,"An Improved Visual Cryptography Scheme for colour images" in IRJET, Aug-2015, Vol. 2, Issue No.5.

[12]]M.Karolin, Dr. T. Meyyapan,"RGB based secret sharing scheme in color Visual Cryptography",in IJARCCE, July 2015 vol. 4,Issue No. 7

[13] Swati Kashyap,Er. NeerajMadan,"A Review on:Network Security and Cryptographic Algorithm" in IJARCSSE, Vol. 5, Issue 4, April 2015.

[14] Rajesh R Mane,"A Review Cryptography Algorithms,Attacks and Encryption Tools" in IJIRCCE, Vol. 3, Issue 9, September 2015.

[15] Sankar Das, SandipanChowdhury and DibyaChakraborty,'Visual Cryptography using Three Independent Shares in Color Images', in IJIRAE ISSN: 2349-2163 Issue 4, Volume 2, April 2015.

[16] Mrs. Smita Desai, Chetan A. Mudholkar, RohanKhade,PrashantChilwant,"IMAGE ENCRYPTION AND DECRYPTION USINGBLOWFISH ALGORITHM" in IJEEE, Vol. 7, Issue 1, June 2015.

[17] Chandan Sharma, Vinod Sharma and AnkushSharma,"Three Quadrant Method for Securing Image by Using Visual Cryptography", CPUH-Research Journal: 2015, 1(2), 59-61,ISSN (Online): 2455-6076.

[18] SrinivasB.L,AnishShanbhag,Austin Solomon D'Souza, "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm" in IJIRCCE, Vol. 2, Issue 5, October 2014.

[19] Aarti, Pushpendra K Rajput," An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding", I.J.Computer Network and Information Security, 2014, 2, 54-60 Published Online January 2014 in MECS, DOI: 10.5815/ijcnis.2014.02.08

[20] ManikaSharma,RekhaSaraswat, "Secure Visual Cryptography technique for color images using RSA algorithm", in IJEIT,April-2013, Vol. 2, Issue No.10.

[21] Pia Singh," IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM IN MATLAB" in IJSER, Vol. 4, Issue 7, July 2013.

[22] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", in IJCSE, Vol. 4 May 2012.

[23] Sozan Abdulla, "New Visual Cryptography Algorithm for colored image" in April 2010, Vol. 2, Issue No.4.

[24] Shruti M. Rakhunde,ManishaGedam," Survey on Visual Cryptography: Techniques, Advantages and Applications", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 06-12

[25] Febin Baby, Arun R, Dr. SuvanamSasidharBabu," ViCry: Visual Cryptography Schemes for Security (An overview of different types of visual cryptography schemes)", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 PP 15-18.