Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Visual Cryptography using Quadri Directional Search Algorithm with Remote Accessibility

S.S. Rajanandan Rao
Dept. of electronics and communication
Dayananda Sagar College of Engineering
Bengaluru, India

Abhishek A.B
Dept. of electronics and communication
Dayananda Sagar College of Engineering
Bengaluru, India

Prajwal B P
Dept. of electronics and communication
Dayananda Sagar College of Engineering
Bengaluru, India

Karan Deshmukh
Dept. of electronics and communication
Dayananda Sagar College of Engineering
Bengaluru, India

Sapna P J
Assistant Professor
Dept. of electronics and communication
Dayananda Sagar College of Engineering
Bengaluru, India

***Abstract*—Gathering intelligence plays a vital role in safeguarding a nation from insurgency and offensive military strikes from hostile countries. It is recommended to provide logistic support to the armed forces constantly thereby keeping them informed of the ground situation and alert them in advance to acquire an advantage. Surveillance is achieved via satellite imaging. Such confidential images captured are to be transmitted in real time securely to avoid any third party from interpreting them. This can be obtained by utilizing Visual Cryptography. Visual Cryptography secret image sharing ensures security of the transmitted information by splitting a secret image into n shares which are owned by n participants to prevent the secret from accidentally being lost. Existing algorithms provide solutions for problems such as secret information leaking from shares, attack on share images and large share image issues but their time complexity is still debatable. Therefore, the proposed Quadri directional search algorithm technique can be implemented for encrypting the information.**

Keywords*—Visual Cryptography, Imaging, Shares, Encryption, Image

I. INTRODUCTION

Secret sharing has attracted attention in the past decades. Contrary to conventional protecting data mechanisms such as data encryptions and data hiding, secret sharing shares data into several parts which are kept by a group of participants to avoid losing data accidentally or intentionally. The concept of secret sharing was proposed independently by Shamir and Blakley. Inspired by Shamir's and Blakley's (t, n) threshold schemes, many scholars began focusing on the study of secret sharing. However, the major drawback of these schemes is that their secret data are integers or texts instead of images. In 1995, Naor and Shamir extended it to secret image sharing which is applied to imagesCryptography is the method of protecting information by making use of a secret key, to ensure only the intended receiver can decrypt it**.** The extension of cryptography upon visual information such as images is known as Visual Cryptography.In visual cryptography, the Cipher Text is called a 'Share'. A share contains only partial information of an image. Hence an image can have 'n' number of shares which can be held by n receivers to avoid the secret from incidentally or intentionally being lost. The QDSA method can be used to share any bank related financial documents, footages of surveillance camera, any information in the crime investigation field, medical field, bank captcha, in military applications by capturing the enemy activities from a camera.

II. LITERATURE SURVEY

Initially Visual cryptography by Moni Naor and Adi Shamir [1] a technique where greyscale images are encrypted into n shares and superimposing the shares gave back the original image. The simplest method of visual secret sharing problem assumes that the message consists of a collection of black and white pixels and each pixel handled separately. Each original pixel appears in n modified versions. (called shares), one for each transparency. Each share is a collection of m black and white subpixels Which are in close proximity to each other so that the human visual system averages their individual black/white contribution. This framework resembles the linear codes, with the important difference that the underlying algebraic structure is a semi-group rather than a group. In particular, the visual effect of a black subpixel in one of the transparencies cannot be undone by the color of that subpixel in other transparencies which are laid over it. This monotonicity rules out common encryption techniques which add random noise to the cleartext during the encryption process, and subtracts the same noise from the ciphertext during the decryption process. Any single share contains 5 black subpixels, any stacked pair of shares contains 7 black subpixels, any stacked triplet of shares contains 8 black subpixels, and any stacked quadruple of shares contains either 8 or 9 black subpixels, depending on where the shares were

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

taken from. It is possible to reduce the number of subpixels from 9 to 8, but then they cannot be packed into a square array without distorting their aspect ratio.

Later Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels by Philip A Eisen and Douglas R Stinson [2] introduced a method known as a threshold visual cryptography scheme (VCS), has the benefit of requiring no cryptographic computation on the part of the decoders. This new definition motivates an examination of minimizing pixel expansion subject to fixing the VCS parameters $">h$ and $">l$. New bounds on pixel expansion are introduced, and connections between these bounds are examined. The best bound presented is tighter than any previous bound. An analysis of connections between (2, $">n$) schemes and designs such as BIBD's, PBD's, and ($">r$, λ)-designs is performed. Also, an integer linear program is provided whose solution exactly determines the minimum pixel expansion of a (2, $">n$)-VCS with specified $">h$ and $>l$. Given a finite set X (of elements called *points*) and integers k, r, $\lambda \geq 1$, we define a *2-design* (or *BIBD*, standing for balanced incomplete block design) B to be a family of k-element subsets of X, called *blocks*, such that any x in X is contained in r blocks, and any pair of distinct points x and y in X is contained in λ blocks.

Further Extended visual cryptography for color images using coding tables by Meera Kamath and Arpita Parab[3] proposed scheme make use of Jarvis error filter, a key table and specialized tables for coding. It works on the same principle as Adi and Shamir's cryptography. There are three steps in the algorithm are Color Halftone Transformation, Encoding and Generation of Shares, Decryption. According to Color Halftone Transformation each input image is decomposed into three constituent planes red, green and blue. Then the halftone technique is applied to each of these planes. By combining these three halftoned planes, a color halftone image is generated. Halftoning is performed using error diffusion. In the decryption process, we stack two or more shares along with the Key Image to reconstruct the secret image. Figure 6 shows an example of decryption with blocks from two shares, Share1 and Share2 and the corresponding block from the Key Image. The block of the stacked image produced contains two subpixels of the same color as the pixel of the secret image and the other two subpixels are black. Since two subpixels out of four in each block will always be of the same color as the pixel of the secret image, 50% of the secret image is retained in the final reconstructed image.

Later RGB based color sharing scheme in color visual cryptography by M. Karolin and T. Meiyappan [4] proposed a method for images with 256 colors which are converted to 16 standard RGB colors format. It generates shares without compromising the resolution. The Floyd-Steinberg dithering algorithm is used to manipulate the 256-color code image to reduce it to 16 standard colors code image. The basic model of visual cryptography for color images consists of three phases. The first phase to realize color visual cryptography scheme is -to print the color in the secret image on the shares directly. It performs larger pixel expansions which reduce the quality of the divided color image. The second phase converts a color image into black and white image on the three-color channels (Red, Green, Blue or equivalently cyan, magenta, yellow) respectively, and then applies the black and white visual cryptography scheme to each of the color channels. This results in decrease of pixel expansion of a greater number of pixels but reduces the quality of the image due to halftone process. The third phases utilize the binary representation of the color of a pixel and encodes the secret image at the bit-level.

III. QDSA TECHNIQUE

Quadri-Directional Search Algorithm (QDSA) technique is used to encrypt secret images into shares by using a sudoku key. This method searches the sudoku key in 4 directions North, South, East and West for the encryption and decryption of the secret image and shares respectively. Also, QDSA is applicable to both colour and greyscale images. This produces high quality images and 100% of the image can be recovered. Advantages here are Pixel expansion is avoided, new keys are generated every time which improves security, Quality of the decrypted image is not compromised, two level security is provided.

IV. BLOCK DIAGRAM

Due to the enormous development in the digital world security plays an important role in transmission of images. Several methods such as steganography, cryptography etc., Visual cryptography is a best technique for security as it allows the visual information to be confidential. Visual cryptography encodes the secret into shares, that are parts of the secret image but do not reveal the secret image visually. The images that are taken as input in the project are gray scale and color images. Hence the block diagram can be divided into two parts- Grayscale image and color image.

A. Grayscale Images

The process of encryption and decryption are explained below with the help of block diagrams. The block diagrams can be split into 4 parts -Conversion, Encryption, Security and Shares.

Transmitter side

The image is first interpreted in the form of intensity levels the image is then converted from base 10 to base 9 format as shown in Fig. 1, the sudoku table is used here since it is compatible with base 9 image. A random sudoku table is chosen for the encryption process, the randomization is done based on the particular minute of that hour. This time stamp is encrypted using a password and sent to the receiver along with the encrypted shares. The shares are generated using the sudoku table. These shares which are in the form of collection of numbers are converted to a picture fat using the image key. This is done by randomly assigning intensity levels of the image key to the coordinates in the shares. Shares generated in this way are then uploaded to the online database, in this project the online database used is Google Firebase. As it can be seen, here the QDSA technique has been seen.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

Receiver Side

The shares are downloaded from the database as shown in Fig. 2. These shares are converted back to the number format by using the image key, it means that the intensity levels are converted to numbers. The image key is obtained from the time stamp sent along with the shares. By using the sudoku key with the three individual shares. First share is used to obtain the first digit of the base 9 number, second and third shares are used to obtain the respective digits of the base 9 number. These three shares in the form of numbers are converted to one image in base 9 format. This image in base 9 format is then converted back to base. Hence the secret image is recovered.

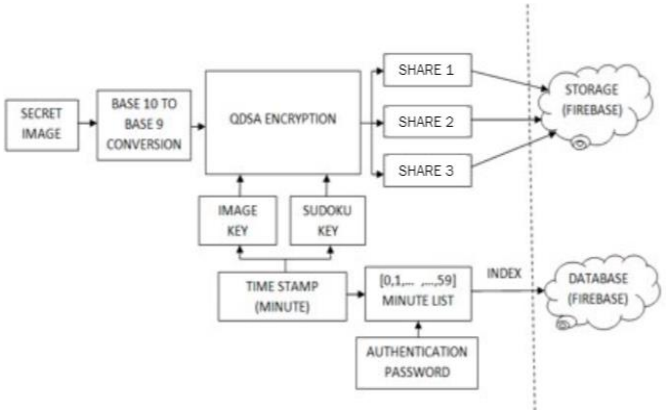

Fig. 1: Transmitter side block diagram for grayscale images

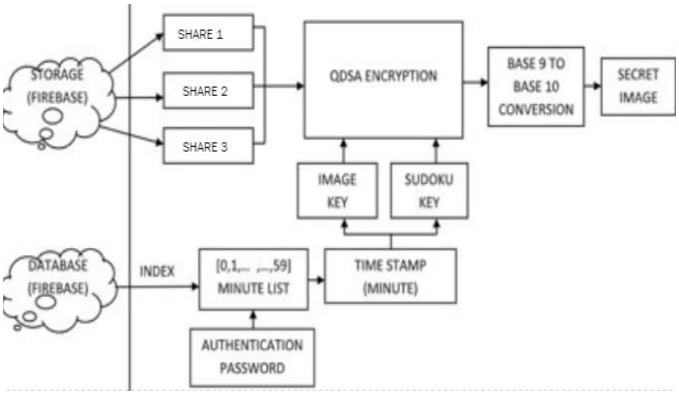

Fig. 2: Receiver side block diagram for grayscale images

B. Color Images

The block diagrams can be split into 4 parts -Conversion, Encryption, Security, Shares. The color images used in the process are in RGB format.

Transmitter side

The image is first interpreted in the form of intensity levels in red, green and blue colors as shown in Fig. 3. These images are then converted to a base 9 format. A random sudoku table is chosen for the encryption process, each image (red, green, blue) is encrypted separately, the randomization is done based on the particular minute of that hour. The time stamp is encrypted using a password and sent to the receiver along with the encrypted shares. This is done by assigning intensity levels of the image key to the coordinates in the shares in a zigzag manner, three shares are produced for each color (three for red, blue and green). These shares which are in the form of collection of numbers are converted to a picture format using the image key. The shares are generated using the sudoku table. Here, 9 shares are generated. Share images generated in this way are then uploaded to the online database, in this project the online database used is Google Firebase.

Receiver side

The shares are downloaded from the database as shown in Fig. 4. These shares are converted back to the number format by using the image key, it means that the intensity levels are converted to numbers. This process is done separately for all the 9 shares and 3 colors. The image key is obtained from the time stamp sent along with the shares. These three shares in the form of numbers are converted to one image in base 9 format. This is done by using the sudoku key with the nine individual shares. First share is used to obtain the first digit of the base 9 number, second and third shares are used to obtain the respective digits of the base 9 number. This process is repeated for the other two colors. This image in base 9 format is then converted back to base 10 image. Hence the secret image is recovered.

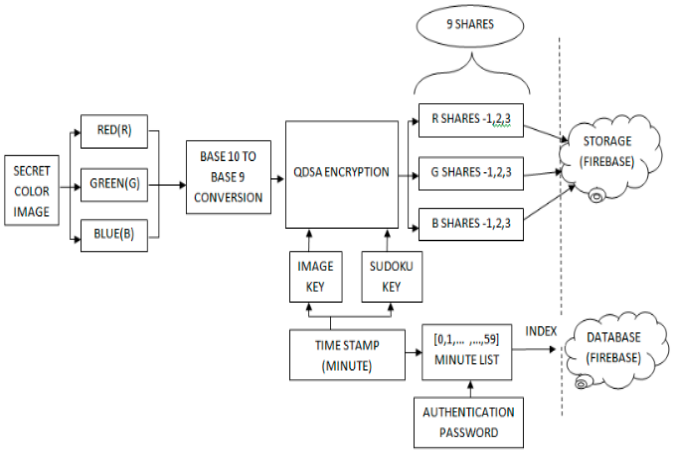

Fig. 3: Transmitter side block diagram for color images

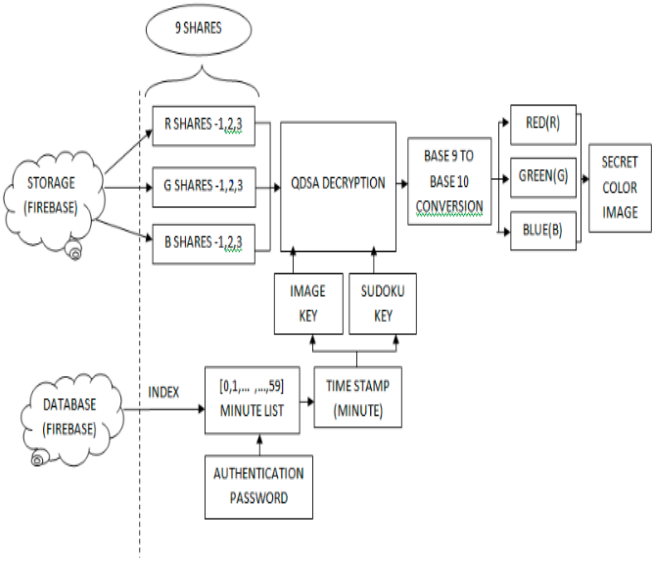

Fig. 4: Receiver side block diagram for color images

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

V. EXPERIMENTAL RESULTS

A. *Grayscale Images*

Shares at transmitter side

This scheme is the most basic one applied on a Grayscale Image which generates three shares for an image. These shares as shown in Fig. 5 are uploaded to Firebase.

Image at Receiver side

The three shares are taken from Firebase and the Secret Image is recovered from the decryption algorithm. The decrypted image is shown in Fig. 6.

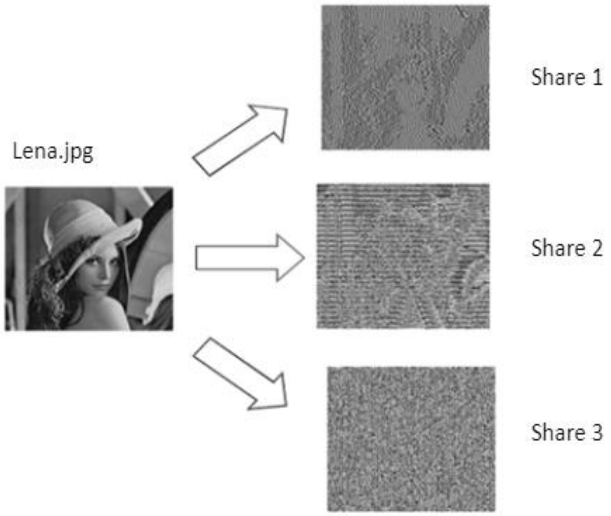

Fig. 5: Encrypted Shares

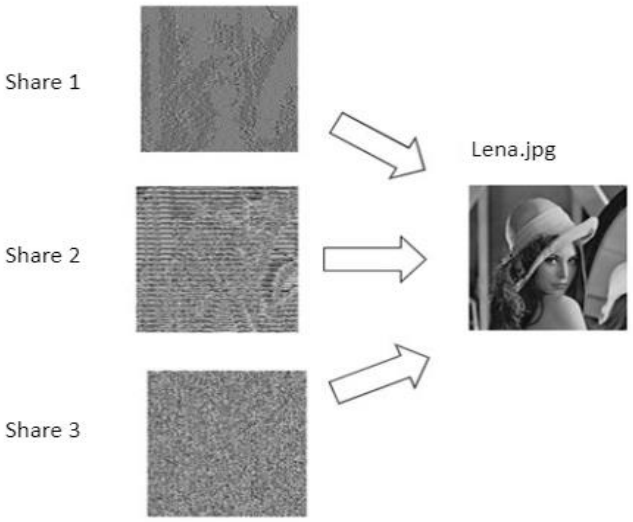

Fig. 6: Decrypted Image

B. *Color Images*

In all the Color Schemes, first the Secret Color Image represented in RGB format is split into three Grayscale images representing the Red, Green and Blue colors respectively. Hence for one Secret Color Image three Grayscale Images are generated.

Shares at transmitter side

This scheme is the most basic one applied on a Color Image which generates nine shares for an image (three shares for each Grayscale image). These shares are uploaded to Firebase. The shares are shown in Fig. 7.

Image at Receiver side

The nine shares are taken from Firebase and the three Grayscale Images are recovered and are combined to get the Secret Color Image from the decryption algorithm. The decrypted image is shown in Fig. 8.

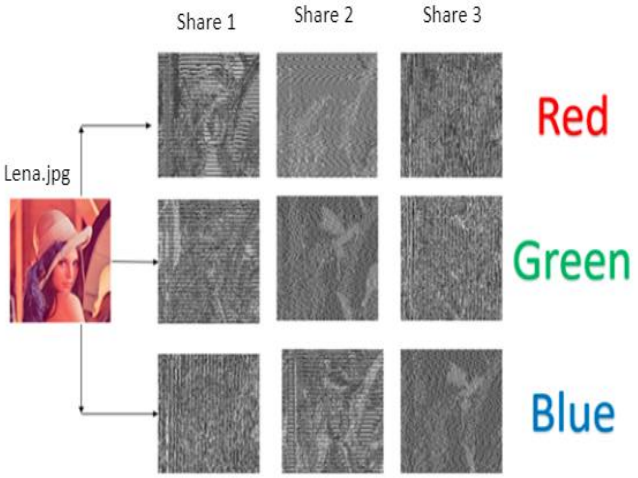

Fig. 7: Encrypted Shares

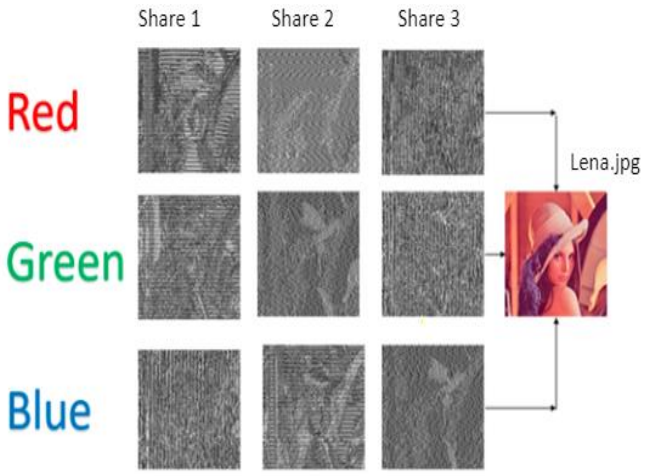

Fig. 8: Decrypted Image

VI. PARAMETERS

PSNR Calculation

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 07, July-2020

PSNR is a measure of how identical two images are with respect to one another.Two identical images have infinite PSNR, and two different images have finite PSNR.The Secret Image sent and the Shares generated are relatively different, hence their PSNR is finite.The Secret Image sent and received are identical hence it's PSNR is infinite.

The TABLE I represents the comparison of PSNR values. Vertically it is compared with different research papers with the proposed scheme. Horizontally different images are taken as input. It can be seen that the proposed scheme has PSNR values less than 10 dB for all the shares.

TABLE I*:* Visual quality of shares obtained from various methods

	Lin and Chan's Scheme [5]		Chin Chen Chang Scheme [6]		Proposed Scheme	
Images	PSNR (dB)		PSNR (dB)		PSNR (dB)	
Lena	40.32 dB	40.45 dB	39.40 dB	39.17 dB	6.70 dB	8.54 dB
Baboon	40.33 dB	40.43 dB	39.34 dB	39.16 dB	9.60 dB	9.80 dB
Airplane	40.35 dB	40.43 dB	39.16 dB	39.18 dB	6.70 dB	8.50 dB
Barbara	40.33 dB	40.46 dB	39.16 dB	39.13 dB	8.91 dB	8.91 dB
Boat	40.29 dB	40.42 dB	39.14 dB	39.17 dB	6.71 dB	8.54 dB

From TABLE II it can be seen that several parameters such as Pixel Expansion, Security and Quality of Recovered Image are improved as compared to the other schemes.

TABLE II: Research Paper Comparison

	Moni Naor and Adi Shamir [1] (Greyscale)	Philip A. Eisen and Douglas R Stinson [2] (Greyscale)	Meera Kamath and Arpita Parab [3] (Color)	M. Karolin and T. Meyyapan [4] (Color)	QDSA scheme (Grayscale and Color)
Pixel Expansion	High	Low	Low	Low	Nil
Security	Low	Moderate	Moderate	High	High
Processing Time	Low	Moderate	Moderate	High	Moderate
Quality of Recovered Image	Low	Moderate	High	High	High

VII. CONCLUSIONS

Visual cryptography is a very broad field which has a great scope in the future for development and research. In this project we have implemented visual cryptography on grayscale and color images. The various stages were implemented in various phases of the project. The algorithm was implemented to grayscale images in the first phase, color images in the second phase, finally the user interface was developed in the third phase. The Quadri-Directional Search Algorithm is proposed using a sudoku table to encrypt the given grayscale image or color images. A second step to the encryption process in which the image key matrix is used to map the sudoku key value to an intensity level in the image key matrix. We also extended the algorithm to encrypt color images by separating the red green and blue intensities of the pixels. A user interface has been developed to access the images. Here is where the project can be developed. The user interface can be further improved to include many other features. The remote accessibility can be improved by adapting the code to a mobile environment. The benefits in the QDSA scheme are there is no pixel expansion hence the quality of the recovered image is high. Since dynamically generated Sudoku keys and Image keys are used the security is high.

VIII. REFERENCES

[1] Moni Naor, "Visual Cryptography", Eurocrypt, Israel, DOI: 10.1007/BFb0053419, 5471098, 1995.
[2] Philip A. Eisen, Douglas R. Stinson, "Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels", Designs Codes and Cryptography, Netherlands, Volume: 25, Issue: 1, Pages: 15-61, 2002.
[3] Meera Kamath, Arpita Parab, Aarti Salyankar, Surekha Dholay, "Extended visual cryptography for color images using coding tables", International Conference on Communication, Information & Computing Technology (ICCICT), India, DOI: 10.1109/ICCICT.2012.6398090, Pages 1-6, December 2012.
[4] M. Karolin, Dr.T.Meyyappan, "RGB Based Secret Sharing Scheme in Color Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering, India, ISSN: 2319-5940, Volume: 4, Issue: 7, July 2015.
[5] P.Y. Lin, C.S. Chan, Invertible secret sharing with steganography, Patt. Recog. Lett. 31 (2010) 1887–1893.
[6] Chin-Chen Chang, Ngoc-Tu Huynh, K. Bharanitharan, "Quadri-directional searching algorithm for secret image sharing using meaningful shadows", Elsevier, 2015.
[7] Anjney Pandey, Subhranil Som, "Applications and usage of visual cryptography: A review", IEEE, Electronic ISBN: 978-1-5090-1489-7, 19 December 2016.
[8] T. V. S. Kiran, K. Rajani Devi, "A Review on Visual Cryptography Schemes", Journal of Global Research in Computer Sciences, 2012.
[9] Ms. Bhawna Shrivas, Prof. Shweta Yadav, "A Survey on Visual Cryptography Techniques and their Applications", International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1076-1079.
[10] Naoki Kita and Kazunori Miyata, "Magic sheets: Visual cryptography with common shares", Computational Visual Media springer link Volume 4, Issue 2, pp 185–195, June 2018.
[11] Trupti Patel and Rohit Srivastava, "Hierarchical visual cryptography for grayscale image", IEEE Online International Conference on Green Engineering and Technologies (IC-GET) 2016.
[12] Ranjith.R, Supreeth S, Ramya R, Ganesh prasad. M, Chaitra Lakshmi L, "Password Processing Scheme using Enhanced Visual Cryptography and OCR in Hybrid Cloud Environment", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249–8958, Volume-8, Issue-5S, May, 2019.
[13] R. M. Shiny, P. Jayalakshmi, A. Rajakrishnammal , T. Sivaprabha and R Abirami "An efficient tagged visual cryptography for color images", IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) 2016.
[14] Young-Chang Hou, "Visual cryptography for color images," Pattern Recognition, Vol. 36, No. 7, pp. 1619-1629, 2003.
[15] Inkoo Kang, G.R. Arce, and H.K. Lee, "Color Extended Visual Cryptography using Error Diffusion," 2009.