*ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015*
International Journal of Innovative Trends and Emerging Technologies

# NATURAL VISUAL SECRET SHARING SCHEME FOR SHARING MULTIPLE FORMS OF IMAGES IN A NETWORK

D.PAVITHRA. M.E.,
Department of Computer Science and Engineering
DMI College of Engineering, Chennai, India
E.mail:pavithraddivya@gmail.com

M.FERNI UKRIT, Assistant Professor,
Department of Computer Science and Engineering
DMI College of Engineering, Chennai, India
E.mail:fernijegan@gmail.com

***Abstract*— The mainstay of this project is to introduce a scheme for sharing various types of images through the network, schemes such as visual secret sharing scheme used only unique or single image that would be subdivided and sent through the network which had great drawback in terms of transmission risk, the images were subjected to high pixel expansion and poor display quality. Hence the natural visual secret sharing scheme which uses multiple images that are combined together and then sent from a sender to a receiver. here the encoding process includes the combining of all n shares and decoding is done through human visual system. Major processing here includes feature extraction, the hiding process of steganography and QR code that serves the purpose of high security. Both pre-processing and post processing operations are carried out both at sender and receiver side.**

***Index Terms*— Natural visual secret sharing scheme, feature extraction, steganography, QR code.**

## I. INTRODUCTION

Latest trends in internet has developed information sharing and made one closer to the other .In the course of time security plays a huge role for sharing this information, this makes many institutions, organizations to spend large amount of money for the purpose of security. Generally secret information that is to be sent is concealed by using the methods of cryptography, this requires high computation cost for its encryption and decryption processes. A new technique was introduced to overcome such problems.

*Visual cryptography* is a new encryption technique that splits an image into n shares any user who has all the n shares only will be able to obtain the information by decoding using human visual system. the scheme that is used for distributing and delivering images is termed visual secret sharing (VSS)scheme. this scheme suffers from high transmission risk, that is since the images are subdivided there are large chances for the images to be lost in the network. it also affects the pixel expansion of images as well as its display quality. The natural visual secret sharing(NVSS)scheme is defined as how an user sends a secret image securely in a network. this scheme combines one or more images to the secret image, the images that are combined with the secret image are known as natural shares. Considering the aspects of high transmission risk ,corruption by unauthorized users this scheme serves at its best. The natural visual secret sharing scheme uses multiple forms of images namely the natural shares these shares could be of any form namely printed or digital. printed images include hand-painted pictures, flysheets. Digital images include any image captured via digital camera or smart phones. The secret image combined along with the natural shares is subjected to various techniques namely feature extraction, steganography for hiding purpose and QR code formation.

The following are the contributions made in the proposed work :

1. The main aim is to reduce the transmission risk of shares by using different forms of media generally termed here as natural shares, the shares include digital or printed images, these natural shares have low transmission risk than noise-like or meaningful shares.
2. The display quality of true-color natural images is greater than that of halftone cover images.
3. The usage of QR code helps to hide the generated share in printed media, the code carries meaningful information and can be read by devices such as smart phones and barcode readers.
4. Pixel expansion is a major drawback that has been addressed here, comparison of secret image and recovered image is done.

In Section 2, literature survey on various visual secret schemes are presented with the focus of reducing transmission risk in a network and enhancing the display quality of images. In Section 3, a system model encompassing a natural visual secret sharing scheme is presented. In Section 4, the proposed algorithm for encryption/decryption ,feature extraction and QR code is presented. In Section 5, the results and implementation of proposed scheme for reducing the transmission risk ,enabling good display quality of images are presented and discussed. In Section 6, provides concluding remarks and the future enhancement.

## II. LITERATURE SURVEY

The major technique used here is the probabilistic method ,in which a basic matrix is being constructed, though revealing information becomes hard the size of the information can be easily guessed. Separate algorithm for decryption is used to obtain the information[1].

Extended visual cryptography(VC)[2],makes use of three images as input and the output consists of two images, the final image is reconstructed based on the two output images obtained by printing them onto transparencies and stacking them. The main disadvantage is that due to the transformations in pixel intensity it reduces the contrast of images. Meaningless shares are constructed using optimization techniques, along with cover images being added in each share by using a stamping algorithm, the term General access structures in visual cryptography[3], can be used to perform encryption by dividing into shares, the major problem is that each encryption phase is less coherent in nature. The number of shares to be used is set as the decryption condition which may vary it also suffers from a major drawback that leads to the modification of display quality of cover images.

Highly efficient encryption scheme[4],is being used so that multiple images can be combined and sent easily in a network here the method used is the hybrid encryption procedure which is used to design a codebook that is free of pixel expansion and a randomly generated amount of pixels is being added, the major drawback is that storing large number of pixel value reduce the quality. General visual cryptography schemes uses either threshold access structures or general access structures[5] ,a scheme that supports both is termed as a good one, here the general access structures are not well defined, a set of column vectors is used for encrypting the secret pixels followed by the application of simulated annealing algorithm, the major drawback defined here is that it uses blackness as one of its criteria to enhance the display quality of images, that is higher the blackness the contrast value decreases accordingly .Thus the problem of pixel expansion in general access structure is highly not addressable.

Threshold visual cryptography[6],scheme is defined as that which can be used to generate n shares, such that the number of shares used could be only k shares, this scheme is used for encoding binary images where the reduction of pixel expansion improves its display quality, a basic optimization model is being specified here, along with the specification of developing an simulated-annealing algorithm. Two types of models are being used here namely a deterministic and probabilistic model, here the blackness of images is highly enhanced where pixels can be easily recovered, the probabilistic model can be used for recovering of pixels perfectly. the terms such as contrast ,blackness and density balance are being addresses here thus pixel expansion and contrast are major drawbacks being addressed. The term embedded extended visual cryptography[7],is used in large for producing random shares and embedding them into cover images, followed by extraction process followed by encryption process and decrypting those images, the cover images or shares are divided into blocks and are carried forward for further processing, the major considerations or drawbacks obtained are pixel expansion at each cover being specified along with the display quality of images that are low in nature. The scheme specified for dividing a secret image that is to sent in a network makes use of shadows[8],which is then embedded in cover images, this produces stego images which are highly different from natural shares, multiple usage of hash functions for storing the framework of shadows, digital signature algorithm is basically used here, two important drawbacks such as integrity and visual quality plays a huge role. The general access structures used for extended color visual cryptography[9],makes n participants, each participant has multiple shares for sharing a single secret image ,a qualified set known as construction set is being formed, they are then subjected to a stamping algorithm to identify the meaningful shares ,selected color images are sent into a stamper for identifying the meaningful color images, major drawback addressed here is how user suffers from identifying meaningful shares. The scheme used for hyper graph colorings[10],that is a hyper graph is specified here, this is a subset of specified values, this scheme makes use of extended visual cryptography scheme, major drawback is that upper bound values and lower bound values are to be notable along with NP-hard problem.

Novel secret sharing schemes[11],for true color images are also being specified, here we combine two schemes such as neural networks and variant visual secret sharing scheme, this uses shares that can be combined and sent from one user to another. The image to be sent is usually defined as a collection of black and white pixels, each pixel[12],is handled individually and it is noted that the white pixel represents the transparent color and black pixel represents zero or it is not visible, drawback of this process is that the decryption process is lossy, which is nothing but the region that is subjected to high contrast, Contrast is very important criteria with visual cryptography because it determines the clarity of the recovered secret image by human visual system. An incrementing VC scheme [15] using random grids, this method has the same incremental revealing effect to the secrets on an image, and the size of each share is the same as that of the original image without any expansion. The smaller size of shares makes their further processing such as storage and printing out more efficient and reliable.

Visual secret sharing technique based on random grid visual secret sharing algorithm[16], this method is that in which the secret image and natural image pixels are divided into two grades grade1 and grade2 depending on which the pixels are moved to its respective grades ,at the receiving end grade1 and grade2 is combined, then moving the pixel in grade1 and grade2 depends on which pixel belongs to which grade ,at the receiving end receiver cannot get the image properly because of the movement of pixel in grade 1 and grade 2 which leads to a change in the time of image pixel value, also affecting the brightness of original image. Trusted third party[13], embed secret image into cover images to generate shadow images, each participant who has the higher number of shadow images only will be able to view the secret images, here the secret image is constructed lossesly, the drawback specified here is that the effects of distortions in images are not specified. The complexity of certain schemes are studied here along with the aspects of including the terms of visual sharing schemes[14],they suffer from high transmission costs ,it also includes multiple techniques such as vector quantization and wavelet transformations.

Here the visual cryptography scheme makes use of n binary shares and then subjected to various encoding operations, here halftoning[17], is combined with the binary images, technique used here is the blue-noise dithering principle, the major drawback of this work is the appearance of images. Alignment of shares during the time of superimposition[20],is carried out here, according to which the source images could only be obtained when the alignment of shares are done perfectly. A scheme that is used to encrypt two images simultaneously, here stacking of two generated shadows[19],to recover the initial or first image is specified followed by the shift in the second shadow horizontally to reveal the second image ,exclusive ex or operation is carried for the initial image followed by the reversible action for the second images, here the quality of images is again a major drawback. The terms such as visual information pixel[18]l, synchronization are being specified here, quality is a major concern. Hence the overall work of natural secret sharing schemes are studied.

## III. SYSTEM MODEL

The system model clearly explains the flow of the entire system used

The system model used for sharing images can be used under various circumstances and solves many problems. The major aspects include:

- Transmission is highly secure.
- Cost for transmission is reduced.
- Images that are used are of high display quality since they are subjected to various constrains.
- Comparison of pixels for both the secret and recovered image is carried out.

The processing begins with the selection of images followed by its preparation.

*Image preparation:*

The process is done both at the sender and the receiver side, it is carried out as follows select the images that are to be used for processing, the selected printed and digital images are subjected to operations such as cropping and resizing to its desired dimensions.

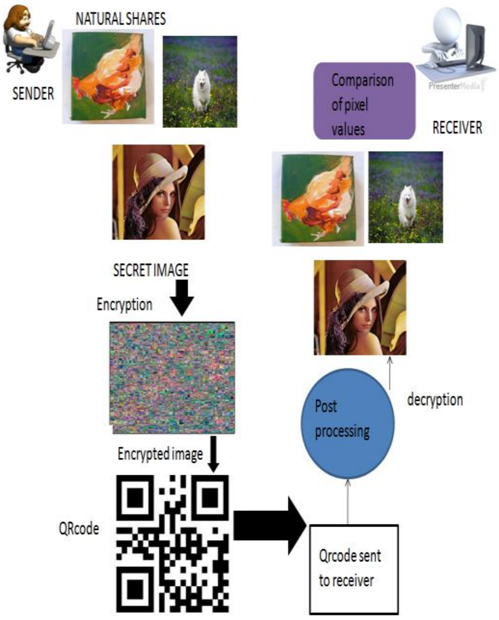


Figure 1.Architecture of natural visual sharing scheme

*Feature extraction process*

This process used as a process of steganography is used to stabilize the pixel values of the feature matrix.

*Encryption process*

The process combines all the images used in the process and forms a encrypted image.

*QR code formation*

The binary values used are converted into hexadecimal values and forms a QR code for hiding the code.

*Decryption process*

This process is done in order to obtain the original images.

*Comparison of values*

The pixel values of both secret and recovered images are compared and no pixel difference is found followed by maintaining the quality of images.

## IV. METHODOLOGY USED

The techniques used for natural visual secret sharing include feature extraction, natural visual sharing encryption process and QR code formation.

### *A. Feature extraction*

This process is used in images extracts features from natural images ,it also extracts a binary feature matrix and checks the pixel values followed by adding noise to the matrix, This is a common steganographic method, called the least significant bit method, that changes the unit values of the binary image data so ones become zeros and zeros become ones. Only a portion of the binary image data needs to be changed to hide another picture,

For example, grid for 3 pixels of a 24-bit image is given:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

For the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(0010110**1 00011101 11011100)**
(1010011**0 11000101 00001100)**
(1101001**0 10101100 01100011)**

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits are to be changed according to the embedded message. On average, only half of the bits in an image will be modified to hide a secret message using the maximum cover ,Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye, Thus the message is successfully hidden.

This can be illustrated by an algorithm namely the feature extraction algorithm, the following are the notations to be used in the algorithm:

- Pixel value **H*x,y*** is the sum of RGB color values of pixel (*x, y*) in natural share N and

  H*x,y*= *R _ px,y+ G _ px,y+ Bpx,y*

- **M** represents the median of all pixel values (H*x*1,*y*1, . . . ,H*xb,yb* )in a block of N.

- ***F*** is the feature matrix of N, *f x,y* belongs to ***F*** denotes the feature value of pixel (*x, y*) If feature value *f x,y* is 0, the feature of pixel (*x, y*)in N is defined as black. If *f x,y* is 1 the feature of pixel (*x, y*)in N is defined as white.

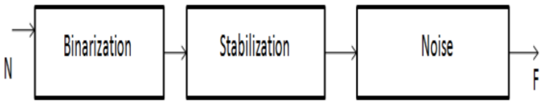


Figure 2 .Flow diagram of feature extraction process

Where, **N** is the natural share ,**F** is the feature matrix.

The following algorithm shows the feature extraction process:

**Step 1:**The natural share is divided into number of blocks of pixels**.**
**Step 2:** For each block calculate the pixel value **H*x,y*.**
**Step 3:** Also calculate the median M.
**Step 4:** The feature value of the pixel is being calculated by using the value of feature matrix.
**Step 5:** If *f x,y* is 1,then x,y in N is termed as white.
**Step 6:**If *f x,y* is 0,then x,y in N is termed as black.
**Step7:**The terms Qc and Qs are found in each black feature pixels and are made white.
**Step 8:**Alter the values of *f x,y.*

**Step 9:** Output the feature matrix F.

The output of the extraction process is sent for visual cryptographic encryption process that is used for combining images without the usage of key, here the major operation performed is the XOR method on all the 24-bit planes of an image.

*B. Image Encryption:*

The encryption process for images uses a different technique than what is used for cryptography, here we consider multiple images that are combined and sent through a network.

An image can be encrypted in the same way that text is encrypted, that is by running a sequence of mathematical operations, on the binary data that comprises an image encryption changes the values of the numbers in a conventional way. A software key is used to unlock the encryption code, and it is created by the same software that combines the picture. The encrypted image and the key are sent to the recipient separately to minimize the risk of an unauthorized person to intercept both. The software key, which is usually a type of password, is given to decipher the encoded image, here in visual cryptography for decoding the image we use the human visual system. The security of the encryption depends on how difficult the encrypted data are to un encrypt.

The algorithm that can be used for performing the encryption process along with steganogaphy,they include both the printed and digital images that are to be used for further processing. The following algorithm explains the process in encryption:

**Step 1:** Initialize by using np and nd printed and digital images.
**Step 2:** The np printed images are subjected to the image preparation process.
**Step 3:** The images used for processing should be of 24-bit/pixel true color images.
**Step 4:** A basic step that is extracting features are carried out.
**Step 5:** Followed by which the swapping of pixel values is performed.
**Step 6:** Finally the feature images and input image are XOR red in every color plane.

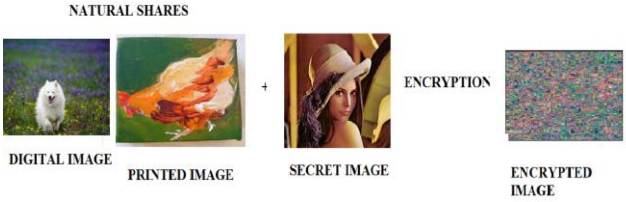


Figure 3.Encryption process

The above figure explains how the natural shares are combined and forms an encrypted image.

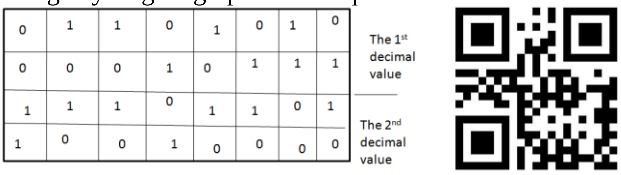
*C. QR code formation:*

The QR code also known as Quick-Response code is used to hide or protect the noisy image obtained. It also includes various processes of steganography for hiding the secret behind images. The code mainly is used for hiding details in printed media.

The QR code consists of a feature matrix, for which the QR code is generated, the hiding process is explained as follows:

**Step 1:** Select the pixels of images for which the QR code is to be formed.
**Step 2:** Transform these values into binary values.
**Step 3:** Represent the binary values in decimal format.
**Step4:** This will be carried for the entire pattern of images.
**Step 5:** Then encode the decimal values into the code.
**Step 6:** Finally the QR code is formed.

The code obtained is sent to the receiver side, along with the collection framework of values, only the keys are extracted and embedded in the code, from which user proves whether he/she is an authorized person or not .Finally decryption process is carried out with the use of human visual system or using any steganographic technique.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

Figure 4.QRcode formation.

## V. EXPERIMENTAL RESULTS AND DISCUSSIONS

The major results found in the proposed work can be listed as follows, the major results include the image preparation process, followed by the feature extraction process, encryption and forming the QR code followed by decryption and comparison of pixel values for both the secret and recovered image.

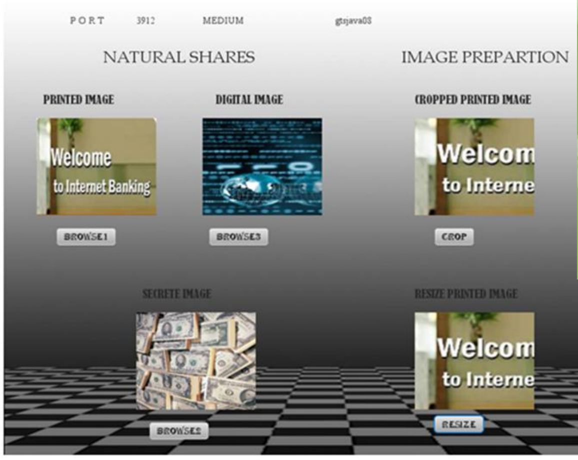


Figure 5.Image preparation process

The feature extraction also termed as the process in which the pixel values are turned from zero to one.

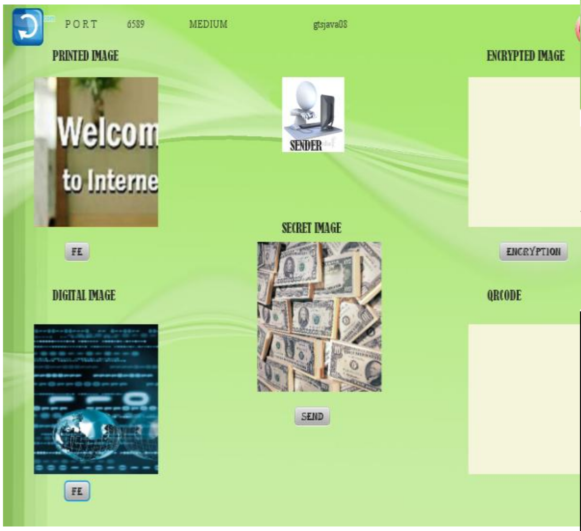


Figure 6.The feature extraction process

The encryption process which can be used to combine the images forming an unique image.

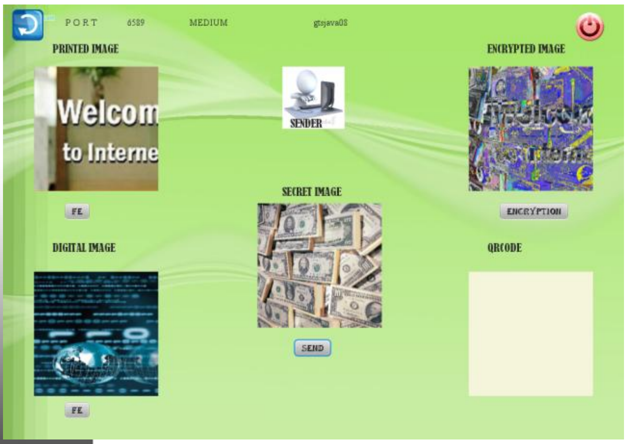


Figure 7.Encryption process.

The QR code is formed in this process, this code plays a major role for hiding the data.

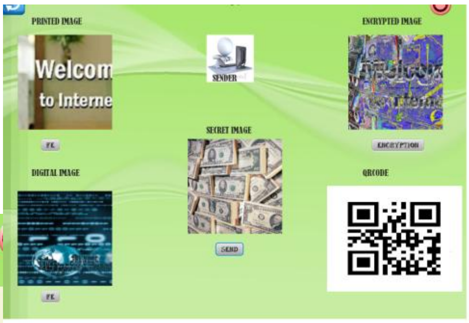


Figure 8.QRcode formation.

After which the decryption process and comparison of pixel values is carried out.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 . | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

The 1st decimal value

The 2nd decimal value

Figure 9..Comparison of values.

## VI. CONCLUSION

Natural visual sharing scheme for digital images is implemented by using various forms of natural shares, steganographic techniques have been used, thus leading to secure transmission of images, and quality of images highly enhanced. Comparison of pixels is done for both secret and recovered images.

## References

[1]. M.Sukukumar Reddy ,S.MuraliMohan , "Visual Cryptogrphy Scheme for Secret Image Retrieval" International Journal of Innovative Research and Studies,Vol2 Issue 6,June 2013.

[2].Mizuho Nakajima Yamaguchi "Extended Visual Cryptography for Natural Images" Department of Graphics and Computer Sciences Graduate School of Arts and Sciences,The University of Tokyo,3-8-1Komaba,Meguroku,Tokyo,Japan 153-8902.

[3].Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures"IEEE Transactions on Information Forensics and Security,Vol 7,NO.1,February 2012.

[4].Kai-Hui Lee and Pei-Ling Chiu, "A High Contrast and Capacity Efficient Visual Cryptography scheme for the Encryption of Multiple Sceret Images"2011 ElsevierB.V 26th Feburary 2011.

[5].Kai-Hui Lee and Pei-Ling Chiu, " Image Size Invariant Visual Cryptography for General Access Structures subject to display Quality Constrains." IEEE Transactions on Image Processing,Vol.22,NO.10,October 2013.

[6]. Kai-Hui Lee and Pei-Ling Chiu, "A Simulated Annealing Algorithm for General Thershold Visual Cryptography Schemes"IEEE Transactions on Information Forensics and Security,Vol 6,No.3,September 2011.

[7].Jerripothula Sandeep ,Abdul Majeed, "Embedded Extended Visual Cryptography Scheme"IOSR Journal of Computer Engineering(IOSRJCE),8727 Volume 8,Issue 1(Nov-Dec 2012)

[8].Z.Eslami*,S.H/Razzaghi,J.Zarepour Ahmadabadi, "Secret Image Sharing Based on Cellular Automata and Steganography"(2009 Elsevier Ltd)

[9].Juby Justin and Giss George, "An Extended Color Visual Cryptography Algorithm for General Access Structures"International Journal for Advance Research in Engineering and Technology,Vol 1,Issue 5,June 2013.

[10].Giuseppe Ateniese, Carlo Blundo,Alfredo De Santis and Douglas R.Stinson, "Extended Capabilities for Visual Cryptography"Department of Combinatorics and Optimiztion,University of Canada ,Waterloo Ontario N2D,3G1,Canada.

[11].D.S.Tsai ,G.Horng,T.H.Chen and Y.T.Huang, "A Novel image secret sharing scheme for true-color images with size constraint"Inf.sci,Vol 179,no.19,pp.3247-3254,Sept 2009.

[12].M.Naor and A,Shamir, "Visual cryptography and advances in cryptology,Vol.950,New York,NY,USA-Springer –Verlag 1995,pp 1-12.

[13].Cheng Guo & Chin-Chen Chang & Chuan Qin, "A novel (n,t,n)secret image sharing scheme without a trusted third party", Springer Science+Business Media New York 2013,29 May 2013.

[14].T.Hoang Ngan Le a,Chia-Chen Lin b*,Chin-Chen Chang c,d,Hoai Bac Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images",Elsevier 2011.

[15].R.Z.Wang,Y.C.Lan,Y.K.Lee,S.Y.Huang,S.J.Shyu and T.L.Chia, "Incrementing visual cryptography using random grids",Optcommunication,Vol.283,no.21,pp.4242-4249,Nov.2010

[16].T.H. Chen and K.H.Tsao, "User-friendly random grid based visual secret sharing"IEEETrans.cir Syst Video Technology,vol.21,no.11,pp.1693-1703,Nov.2011.

[17]. Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography,"*IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453,Aug. 2006.

[18]. I..Kang, G. R. Arce, and H. K. Lee, "Color extended visual cryptography using error diffusion," *IEEE Trans. Image Process.*, vol. 20, no. 1,pp. 132–145, Jan. 2011.

[19].Abhishek Kr Mishra,Ashutosh Gupta,Ashish Kumar, "(n,n)visual cryptography based on alignment of shares", Volume 60,no-18,December 2012.

[20]. Zhi-Hui,Wang Marcos Segalla Pizzolatti and Chin-Chen-Chang ,"Reversible visual secret sharing based on random grid for two-image encryption "International journal of innovative computing ,Information andcontrol,Vol.9,no.4,April2013.