IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 8, Issue 2 (Nov. - Dec. 2013), PP 11-18
www.iosrjournals.org

Key based Visual Cryptography Scheme using Novel Secret Sharing Technique with Steganography

Poonam Bidgar[1], Neha Shahare[2]
[1] *M.E Student, SITS, Department of E&TC, Pune University, Pune, India*
[2] *Asst. Professor, SITS, Department of E&TC, Pune University, Pune, India*

Abstract: *With rapidly growing network, Internet has become a primary source of transmitting confidential or secret data such as military information, financial documents, etc. In such cases, techniques devoted to protect such kind of information are needed and they play an important role in providing confidential and secure transmission over network. Visual Cryptography is also one of them which is used to hide secret visual information (such as image, text, etc) in which secret sharing scheme is used. Secret sharing is used to encrypt a secret image into customized versions of the original image. There are many secret sharing algorithms in literature including Shamir, Blakley, and Asmuth-Bloom to divide the image into no. of shares. These sharing schemes lead to computational complexity and also generate shares like noisy images. Then afterwards Lin & Tsai proposed a scheme which creates meaningful shares but having same computational complexity as like Shamir's scheme. Along with this, in these schemes, as decryption is done using Human Visual system, the secret can be retrieved by anyone if person get at least k no. of shares. To overcome all above problems, we are suggesting one new method in which a symmetric secret key is used to encrypt the image and then secret shares are generated from this image using Novel secret sharing technique with steganography. So, finally this method will produce meaningful shares and use of secret key will ensure the security of scheme. This scheme can become a reliable solution suitable for today's authentication challenges.*
Index Terms: *Visual cryptography, Secret sharing, steganography.*

I. Introduction

In today's information age, security of data has become an emerging area of research that deals with all aspects of secure data communication. The Internet has become a popular communication network where the distribution of multimedia content, confidential data such as military information, financial documents, etc. has become a common practice. But, over Internet the information is viewed to many users. Hence, now the security of visual information has become more and more important in many real applications. To fulfill such an increasing demand of security, many security providing tools are there in this scenario and Visual cryptography is one of them. This is introduced by Naor & Shamir in 1979 to provide confidentiality and security when secret visual information is transmitted through unsecured communication channels. Using secret sharing concepts, the encryption procedure encrypts a secret image into number of shares (printed on transparencies) which can be distributed among group members or transmitted or distributed over number of an untrusted communication channels such that only stacking of these shares can reveal the information otherwise not. Then the idea of secret sharing was also separately proposed by Adi Shamir and G. Blakley in 1979. In 1983 another method of secret sharing was proposed by Asmuth and Bloom. Shamir's scheme is based on Polynomial Interpolation. Blakley secret sharing is based on hyper plane geometry. Asmuth-Bloom secret sharing scheme is based on Chinese Remainder theorem. Then there are many methods to protect sensitive data in image and Steganography is also one of them. This method hides a secret message in a innocent cover medium which could be a digital image, video, audio; etc. but, the weakness of this technique is that an entire secret data is kept in a single cover medium and if this cover medium get lost or corrupted then that hidden data may also get corrupted. In 2004, Lin and Tsai proposed a method that used Steganography for generation of meaningful shares with secret image sharing. This scheme also used polynomial-based secret sharing approach proposed by Shamir which leads to high computational complexity. As the decryption process is done by human visual system, secret information can be retrieved by anyone if the person gets at least k number of shares. So that simple visual cryptography became very insecure.

In this paper, a new idea is suggested which is a visual cryptography method different from any of the methods discussed previously. In this new method, original image having secret information is going through two levels of encryption. In first level, secret image is encrypted by using a symmetric key based visual cryptography resulting into new cipher image which is then divided into no. of meaningful shares by applying novel secret sharing with steganography algorithm. The remaining paper is organized as follows: Section 2 describes related work about various previous visual cryptography schemes. Section 3 describes our proposed

visual cryptography scheme in detail. Experimental results are included in Section 4 and finally, Section 5 draws the conclusion.

II. Related Works

Possible ways to protect secret image based information against interceptor are encryption with shared key, secret sharing of image or hiding image information in other multimedia contents. As our new proposed idea is combination of key encryption based visual cryptography approach and a novel secret sharing with steganography approach we briefly reviewed some of visual cryptography schemes in this section as follows. Previously, Naor and Shamir introduced secret sharing approach in 1979. Afterwards, Asmuth and Bloom proposed another secret sharing algorithm. Shamir's secret sharing scheme is based on Lagrange's Polynomial Interpolation theorem. This scheme divides a secret data image into n number of shares share1, share2……share n and these n shares are Xeroxed onto n transparencies, respectively, and distributed amongst n participants, one for each participant. Such that: i) By superimposing any k or more shares among share i transparencies together can reveal the secret information. ii) Less than k shares reveals no information about the secret share. This technique is called (k, n) threshold secret sharing. The (k, n) secret sharing comes from the concept that k points are necessary to define a polynomial of degree (k−1). Blakley Secret sharing scheme is based on hyper plane geometry. It is known that non-parallel planes intersect at a single specific point. This secret sharing scheme says that: i) Secret is a single point in m-dimensional space. ii) Share corresponds to a hyper plane. iii) Intersection of threshold planes gives the secret. iv) Less than threshold planes will not reveal secret. In Asmuth-Bloom secret sharing scheme shares are created on the basis of Chinese Remainder theorem. In this, shares are generated by reduction modulo operation and the secret is recovered by solving the system of congruence using the Chinese Remainder Theorem. Previously, visual cryptography was restricted to binary images and because of this; it became inefficient in real time applications. Chang- ChouLin, Wen-Hsiang Tsai proposed visual cryptography for gray level images by dithering techniques. A dithering technique is used to convert gray level images into approximate binary images. Then shares are created by applying existing visual cryptography schemes for binary images. The limitation in this is that all generated shares are random patterns carrying no visual information, look like noisy images. This scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256. Halftone Visual Cryptography was proposed by Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo. In this paper, a general framework of halftone visual cryptography is proposed by which visually pleasing halftone shares, carrying significant visual information are generated. Applying the rich theory of blue noise halftoning into the construction mechanism of conventional VC, the obtained visual quality is better than that attained by any other available VC method. Extended visual cryptography for natural images first introduced by Naor which constructs meaningful binary images as shares as shown in fig. 1 and enables the contrast enhancement, where a simple example of (2, 2)-EVCS was presented. This can be treated as a technique of steganography.

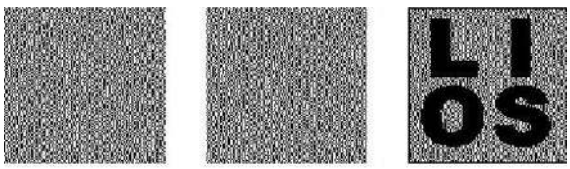

Fig.1. Example of traditional (2, 2)-VCS

There are many EVCSs proposed in the literature. Droste, Ateniese, and Wang also proposed three EVCSs, respectively, by manipulating the share matrices. Nakajima also proposed a (2, 2)-EVCS for natural images. Then afterwards Embedded Extended Visual Cryptography Scheme was proposed by Feng Liu and Chuankun Wu and realized by embedding the random shares into the meaningful covering shares as shown in Fig.2.

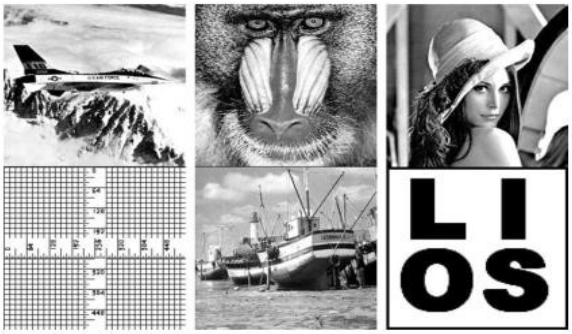

Fig. 2: Original share images (airplane, baboon, Lena, ruler, and boat) and the secret image.

An Extended Visual Cryptography Algorithm for General Access Structures was proposed by Kai-Hui Lee and Pei-Ling Chiu. This approach consists of two phases. In the first phase, they construct meaningless shares using an optimization technique and the construction for conventional VC schemes. In the second phase, cover images are added in each share directly by a stamping algorithm. The experimental results indicate that the display quality of the recovered image is very close to that obtained using conventional VC schemes. Liu, C.K. Wu X.J. Lin, proposed a new approach on visual cryptography for colored images. They proposed three approaches as follows: In first, they realize the color VCS as to print the colors in the secret image on the shares directly similar to basic model. It reduces the quality of the decoded color image. In second, a color image is converted into black and white image or the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels which results in reduction in quality of the image due to halftone process. And in final approach they utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level which results in better quality than first two but requires devices for decryption. Shared Key Encryption of JPEG Color Images was proposed by Subramania Sudharsanan. This paper mainly focuses on {2, 2} shared encryption method for JPEG images. This method creates two shares of JPEG or any format image. This method uses the quantized DCT coefficients in the JPEG representation for generation of shares. These shares are used to reconstruct the original quantized DCT coefficients during decryption. This offers all the compression advantage of JPEG to all the created share images.

III. Proposed Concept

To transmit or store an image in a safer way against unauthorized persons, there are at least three possible major approaches: encryption with keys, hiding the image in other media or objects i.e, steganography, sharing of image among distinct parts i.e. visual cryptography. Combination of these three major approaches is also possible. Secret sharing of image or encryption of image with the help of key produce images which looks like noisy images or textured image. So, there may be chances that attacker may come to know that this image is surely encrypted image or carrying something secret data and if he can't get access to that secret data, he will try to destroy it. For dealing with such problems, one can use steganography which hides the secret information or image into one innocent cover image that the attacker may fails to guess whether this image contains secret information. But, in this entire secret data is kept in single cover image. So, in this also there may be a chance that if this image may get lost or corrupted. For such problem, a method which uses steganography for generation of meaningful shares can be a solution. So, we proposed a new scheme that will overcome such problems associated with secret image encryption. Objective of proposed scheme is to design an encryption/decryption algorithm that efficiently provides high level security for visual information from illicit attacks.

3.1. Encryption Process:

The encryption process involved in our proposed scheme is as shown in Fig.3 which includes firstly encryption of secret image by symmetric key based visual cryptography algorithm which results in cipher image which looks like noisy image and then secondly, by applying secret sharing algorithm with steganography to key encrypted image which results in meaningful shares. Advantage of this combined version of two schemes is that key encryption before secret sharing of image will give additional security and use of steganography in secret sharing can provide additional security as it befools the attacker's eye without computational overhead. In Encryption process, the secret image is first of all treated with symmetric key. This symmetric key is to be generated with the help of symmetric key generation algorithm. After applying key, cipher image is generated which is then divided into n number of meaningful shares by applying Novel secret sharing with steganography algorithm.

3.1.1. Symmetric key generation:

Input to this algorithm is original secret image of size n*m, any other sample image and output will be generated symmetric key which is then used for further part of encryption process. Algorithm used for generation of symmetric key is described as follows:

Step I: Take an image other than original secret image as input. Calculate Height (h) and Width (w) of the image and store it in two or three dimensional image.

Step II: Take a block of any size (e.g. - 4X2, 3X3, 4X3) with elements from array starting from left.

Step III: Initialize an array of size n*m*block size to hold the key declared as Binary_Value and assign the value of elements to zero initially.

Step IV: Now, assume the value of parameter Temp_Value and generate new value of element of array Binary_Value by following steps: Consider, x = 1-2* Temp_Value* Temp_Value. Calculate the value of 'x'. If

value of 'x' is greater than 0 then assign the value of first element of array Binary_Value as 1 otherwise assign it as 0. Now, Temp_Value is equal to x and repeat this procedure for further elements of array Binary_Value.

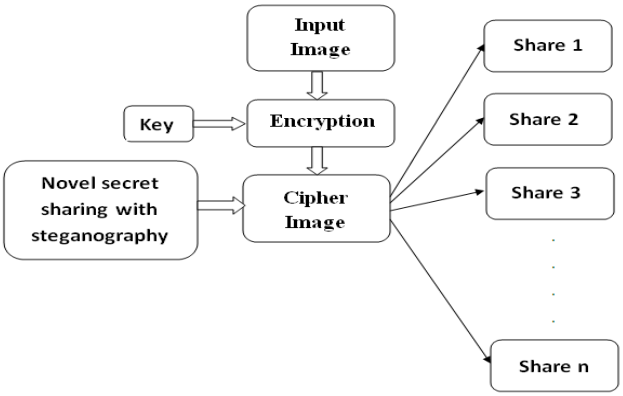

Fig.3. Encryption Process

Step V: Create key array using a repetitive sum method using the formula as:

For i goes from 1 to n*m

For j goes from 1 to block size

do Key[i] = Key[i] + Binary_Value [i*j] * 2 ^ (j-1).

Step VI: Arrange the value of elements of the key array using the principal diagonal approach and generate a two dimensional array Final_Key having n number of rows and m number of columns.

3.1.2. Encryption of Image by generated key:

In this step, Input is original secret image to be encrypted and output will be Encrypted image. Algorithm for image encryption is described as follows:

Step I: Perform bitwise XOR operation between original secret image to be encrypted and generated two dimensional Final_Key array.

Step II: Generate Cipher_Image from step I and print it. This encrypted image will look like noisy image.

3.1.3. Secret Sharing of the Encrypted Image:

In this, generated Cipher_Image by applying symmetric key is taken as input image. By appearance of this Cipher_Image interceptor may come to know that this can be encrypted image and he will try to get data from it. To deal with such case, our proposed scheme use steganography which can hide image shares into cover photo which can make interceptor fail to guess whether this image has hidden some secret data. For this, different masks are to be generated for different shares.

3.1.3.1. Algorithm for designing the masks for n shares with threshold k.

Step I: Get the value of n and k from user and form a matrix of dimension nCk-1 × n by listing all row vectors of size n having the combination of (k-1) numbers of 0's and (n-k+1) numbers of 1's.

Step II: Transpose the matrix generated in Step-1.

Each row of this matrix will represent the individual mask for n different shares. Thus the size of each mask is nCk-1 bits, i.e. the size of the mask varies with the value of n and k. Now, use each row of this matrix for generation the corresponding share.

3.1.3.2. Actual stepwise protocol for image secret sharing scheme.

Input to this step is a key encrypted secret image i.e. Cipher_Image of size n*m generated from subsection3.2 and output of this step will be n meaningful stego share images.

Step I: The mask pattern is placed repeatedly on the secret image. The bytes corresponding to 1 in the mask are kept as it is and the bytes corresponding to 0 in the mask are replaced by 0.

Step II: **S**elect a pixel (say A) from cover image consisting of three bytes for RGB values from the corresponding cover image then insert eight bits of masked byte (say B) into pixel byte image in such a fashion like as shown in fig.4. This forms first stego share image

Step III: Repeat these two steps with all other mask patterns to form other stego share images respectively. So, finally Shares of key encrypted Cipher_Image covered with innocent covers will be created by above mentioned algorithms and they will be ready to send to intended receiver.

3.2. Decryption Process:

At intended receiver, when that n no. of stego share images will get received then after decoding of stego share images will be carried out and original secret image will be recovered. Thus, decryption process consists of steps same as performed in encryption process but exactly in reverse order. In Decryption process, out of n received stego share images firstly select any k no. of share images which are to be stacked.

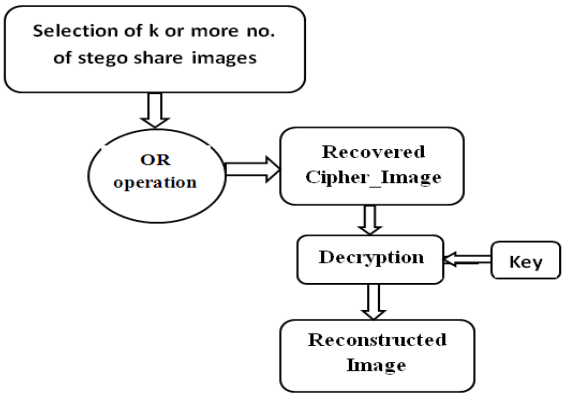

Fig.4. Decryption process

3.2.1. Extraction of share bytes from stego share images:

Input to this algorithm is **n** no. of stego share images and Output will be recovered Cipher_Image.

Step I: First select any k or more no of stego share images. **S**elect the corresponding pixel and extract the share bytes Bi where i= 1, 2, k from the selected k stego share images.

Step II: **P**erform OR operation between these k extracted share bytes we get the corresponding secret byte. Thus, the secret byte is Bs = B1 OR B2 OR - - - OR Bi OR - - - OR Bk

Step IV: Repeat Step II & III with all pixels of k stego images to get back the secret image of dimension*m. Finally, the original lossless Cipher_Image will get recovered by this algorithm**.**

3.2.2. Decryption using key:

Step I: The recovered Cipher_Image is taken as input Generate the key again for decryption process by using key generation step as per 3.1 algorithm explained above and retrieves Final_Key array back in this step..

Step II: Follow XOR operation in between recovered Cipher_Image pixel array and Final_Key array. By this, finally we will get the original secret image at receiver side.

IV. Experimental Results

As per proposed scheme, in encryption process, the original secret image is treated with symmetric key in first step. Leena.png is used as test image for verifying productivity of algorithm. Input to encryption can be any secret image either gray scale, bitmap or color image. For example we considered Leena image of dimension 512x512 as shown below in Fig.3 for conducting experiments. We consider block size of 4x2 and temp value of 0.5155 for key generation. After performing bitwise XOR operation between input secret image i.e. leena.png in our experiment and generated key the output Cipher Image is as shown below in Fig.6:

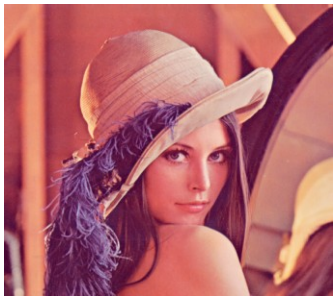

Fig.5. Input secret Image

For evaluating results we had done bitwise XOR between Cipher image and Key array at this phase of encryption process. By this we got original secret image back. These algorithms are implemented by using MATLAB R2010a software. Now, in next step, after applying Novel secret sharing algorithm with steganography as discussed in section 3.1.3 to this Cipher_Image meaningful stego shares will be created as like

shown below. In decryption process, get the value of no. of shares (n) and threshold (k) as input from user. Then after this perform operations as per the algorithm discussed in section 3.2.1 to get Cipher_Image. Output of this i.e. that recovered Cipher_Image will be like this as shown below in Fig.11.

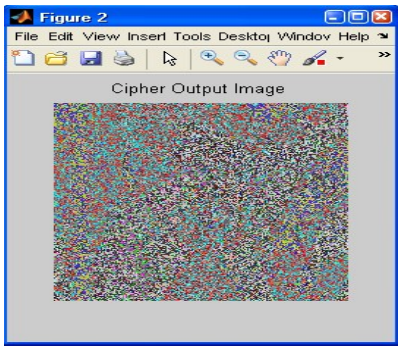

Fig.6. Cipher_Image

For e.g. consider, No. of shares created: n=4. For example, stego share images that will be created can be like these as shown below (see Fig 7 to Fig.10). These images are the example of Stego share images that will be output of Encryption process and will be given as input to decryption process.

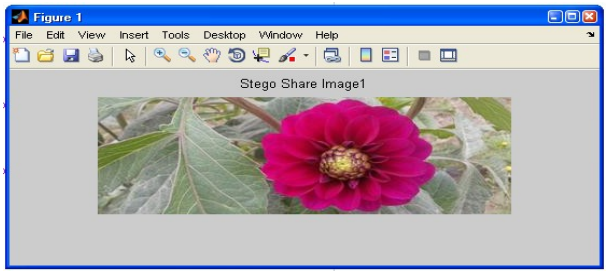

Fig.7. Stego Share Image1

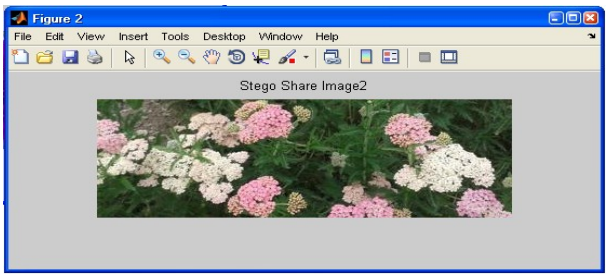

Fig.8. Stego Share Image2

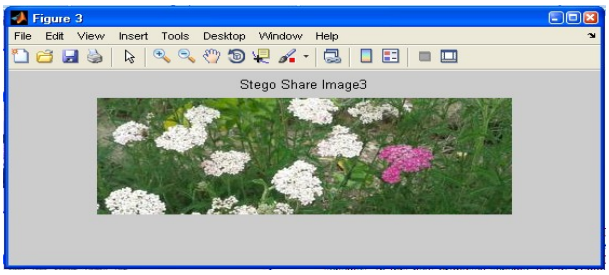

Fig. 9. Stego Share Image3

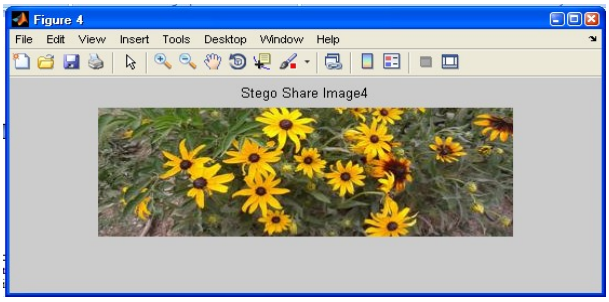

Fig.10. Stego Share Image4

Now, consider, at this stage, take input data from user for Example: Minimum No. of shares required (threshold) =3, Shares inputted: Share1, Share3, and Share4. Then, Reconstructed Cipher_Image Image from shares will be like this as shown in Fig.11. Now, final step of decryption will be decryption with key. Generate the key and then after performing XOR operation between recovered Cipher_Image pixel values and Final_Key array we will get original secret image as shown in fig.12.

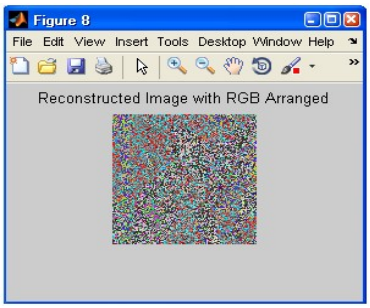

Fig.11. Recovered Cipher_Image

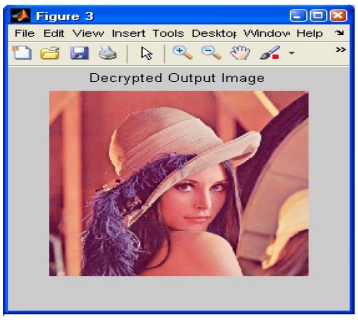

Fig.12. Reconstructed secret image

V. Conclusion

Visual Cryptography is an exciting area of research where exists a lot of scope. We have proposed a new method for visual cryptography different from any other previous schemes. In this new proposed scheme, use of Symmetric key is suggested in first level of encryption process of secret image which will offer additional security. And then we are going to use novel secret sharing with steganography for the creation of shares of this encrypted image which will be meaningful shares instead of having noise like shares. So, because of meaningful shares attacker may fails to guess whether these images contain any secret information. To best of our knowledge this scheme can be a very effective solution in providing security to secret images from illicit attacks. Use of secret key makes it more secure and reliable.

Acknowledgment

The authors gratefully acknowledge all those who have helped in making of this review paper successfully. As, this review process of this paper was carried out at Sinhgad Institute of Science & Technology, Pune. So, special thanks to Head of Computer Department, Principal and Management of SITS, Pune.

References

[1] Prabir Naskar, Ayan Chaudhuri, Atal Chaudhuri **"Image Secret Sharing Scheme Using a Novel Secret Sharing Technique with Steganography ",** IEEE CASCOM Post Graduate Student Paper Conference 2010, Kolkata, India,Nov. 27, 2010, pp-62-65.

[2] Satyendra Nath Mandal, Subhankar Dutta and Ritam Sarkar, **"Block Based Symmetry Key Visual Cryptography",** I. J. Computer Network and Information Security, 2012, 9, pp-10-19.
[3] Feng Liu and Chuankun Wu, Senior Member, IEEE **"Embedded Extended Visual Cryptography Schemes"** IEEE Transactions on information forensics and security, vol. 6, no. 2, June 2011, pp-307-322.
[4] A. Shamir, **"How to share a secret,"** Proc. Comm. ACM, vol. (2), 612-613, 1979.
[5] G. Blakley, **"Safeguarding cryptographic keys,"** Proc. the National Computer Conference, NJ, USA, 1979.
[6] C. Asmuth and J. Bloom, **"A modular approach to key safeguarding"**, IEEE Transaction on Information Theory, 29(2), 1983, pp-208-210.
[7] C.C. Lin and W.H. Tsai, **"Secret image sharing with steganography and authentication"**, Journal of Systems and software, vol. 73, no. 3, 2004, pp. 405-414.
[8] 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, pp-219-229.
[9] Subramania Sudharsanan, Senior Member, IEEE, **"Shared Key Encryption of JPEG Color Images",** IEEE Transactions on Consumer Electronics, Vol. 51, No. 4, NOVEMBER 2005, pp-1204-1211.
[10] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee **"Color Extended Visual Cryptography using error diffusion"** Korea Advanced Institute of Science and Technology, pp- 1473-1476, ©2009 IEEE.
[11] Amos Beimel, **"Secret-Sharing Schemes: A Survey",** Department of Computer Science, Ben-Gurion University, Beer-Sheva, Israel.
[12] Pavan Gupta, Naveen Hemrajni, Savita Shiwani, Ruchi Davey, **"Halftone based Secret Sharing Visual Cryptographic Scheme for Color Image using Bit Analysis"**, Jan 2012, pp- 17-22.
[13] Chin-Pan Huang, **"A New Sharing Secret Algorithm in Stego Images with Authentication",** ICICS 2009, pp-72-76, IEEE.
[14] Chin-Pan Huang, **"A New Scheme of sharing secrets in Stego images with Authentication",** ICIP 2009, IEEE, pp-1269-1272.
[15] Yu-Ting Chen, Cheng-Hsing Yang, Shiuh-Jeng Wang, **"Secret Embedding and Reconstruction for Authentications in Steganography upon Secret Sharing Systems"**, 2010 IEEE, pp-42-48.
[16] Piyush Marwaha, Paresh Marwaha, **"Visual Cryptographic Steganography in images",** 2010 Second International conference on Computing, Communication and Networking Technologies, pp-53-58.
[17] Chi-Shiang Chan, Ping-En Sung, **"Secret Image Sharing with Steganography and Authentication using Dynamic Programming Strategy",** 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, pp-382-385.
[18] Peng Li, Peijun Ma, Xiaohong Su, **"Image secret sharing and hiding with authentication"**, 2010 First International Conference on Pervasive Computing, Signal Processing and Applications, pp-367-370.
[19] J.K. Mandal, S. Ghatak, **"Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography (SITMSVC)"**, IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, MIT, Anna University, Chennai. June 3-5, 2011, pp-263-268.
[20] Liu Shi, Fengyong Li, Yuejun Chen, Xinpeng Zhang, **"Steganographic Embedding in JPEG Images with Visual Criterion"**, 2011 IEEE, pp- 743-746.