DIGITAL DATA SECURITY USING VISUAL CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES: AN EXTENSIVE REVIEW

[1] Jahnavi S, [2] Dr.C.Nandini

[1] Assistant Professor, [2] Professor and Head Computer Science & Engineering Department,
Dayananda Sagar Academy of Technology and Management, Bangaluru -82
[1]Department of Computer Science & Engineering,
[1] Dayananda Sagar Academy of Technology and Management, Bangaluru, India

Abstract : ***Data or information is very crucial to any organization or any individual person. The communication media i.e. internet through which we send data may not be secure every time so there is a need of other methods of securing data, Thus Information hiding becomes more necessary. Information hiding includes Cryptography and Steganography techniques. Cryptography technique was created as to secure communication privacyness and regard to this various methods to encrypt and decrypt secret message has been developed. It is also important to keep the existence of the message secret so with this intension steganography method is used. This paper enumerates advantage and disadvantage of methods implemented in existing work discussed in survey of visual cryptography and steganography techniques with their applications which has to be carried in further Research filed.***

IndexTerms - Visual Cryptography, Steganography, Shares, LSB, PSNR (Peak Signal to Noise Ratio), Secret sharing.

I. INTRODUCTION

With brisk development of technology in internet, various information from different sources is carried over the internet. The data or information can be confidential, personal, and sensitive. Due to security threat issue in transmitting user personal information, data related to military or sensitive data. Data Security must be taken into consideration because hacker can use various methods and steal such high value assets which results in major capital, or personal thrashing.

In Cryptography the format of the original information is transformed in to a format that only desired recipient can read. It protects information from other people from security perspective. Visual cryptography was developed in 1994 by Naor and Shamir to eradicate the habit of using decryption key in the process of secured information transformation.

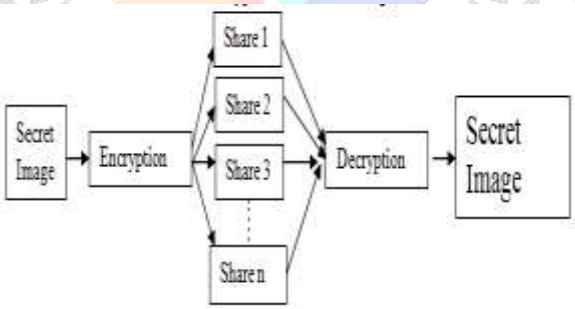

Figure 1.1a: Visual Cryptography Process

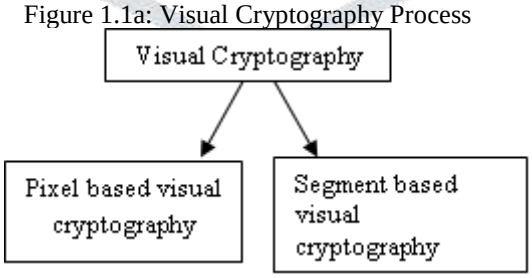

Figure 1.1b: Visual Cryptography methods

At the sender side the original data or information is divided in to shares and transmitted over the network. The receiver on superimposing the shares the original image or information is retrieved as shown in Figure 1.1. With Single share actual or original information cannot be retrieved.

There are two methods in Visual cryptography Pixel based and segment based as shown in Figure 1.1b. In first method of pixel based visual cryptography pixel of the original image is divided into shares, these shares are also called transparencies. The original data is retrieved on stacking shares together. The secret image is converted into monochrome image and then is split into two transparencies, which has pair of pixels for every original image pixel. The pixels are shaded black and white based on the pixel of original image. If the original image pixel is dark(0/) then pixel in shares must be compl□mentary i.e. and the other . If it is □hite(1/ ■)□both should be or both■□ . ■ □ ■ ■□

In Segment based visual cryptography encryption process is based on segment based, it is not based on pixel based. Digits from 0-9 and A-Z is used to represent Message by an LED Display. In Segment based messages are represented by numbers and literals. Example bank

account number, passwords of any websites or shopping sites. Steganography is an invisible communication art achieved by an act of hiding information in other information, which doesn't reveals the existence of information as shown in Figure 1.2 a & b [1].

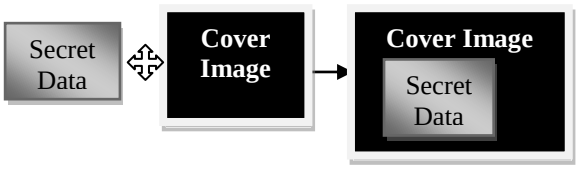

Figure 1.2 a: Encryption process in steganography

Figure 1.2 b: Decryption process in steganography

This paper section organized as follows: Section II briefs about Visual Cryptography Techniques. Section III gives overview on Steganography Techniques. Section IV analysis of combined VCS and Steganography techniques system. Section V Conclusion.

II. OVERVIEW ON VISUAL CRYPTOGRAPHY TECHNIQUES

Author Name	Title and Year	Method	Disadvantage/Problem
Naoki Kita, Kazunori Miyat [2]	Magic sheets: Visual cryptography with common shares 2018 [2]	EVCS with Common Share, share optimization algorithm	Pixel Expansion, Demonstrated for (2, n)-EVCS , has to w.r.t (k, n)EVCS More time consuming in decryption phase, Leakage of information
Yamini Ravella, Dr.Pallavi Chavan [3]	Secret Encryption Using (2, 2) Visual Cryptography Scheme with DCT Compression 2017 [3]	(2, 2) VCS with DCT	Loss of Information
K. Shankar, P. Eswaran [4]	RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography 2017 [4]	Elliptical curve cryptography method	Has to Minimize Mean square error(MSE), To maintain the PSNR on attacks
Trupti and Rohit [5]	A New Technique for Color Share Generation using Visual Cryptography 2016 [5]	Gray share generation algorithm	Security increases with shares. All shares are required to retrieve information
Shiny,P.Jayalakshmi A.Rajakrishnammal, Sivaprabha Abirami [6]	An efficient tagged visual cryptography for color images 2016 [6]	Steinberg error diffusion and Floyd scheme	Very Poor image quality with loss of information
Trupti and Rohit [7]	Hierarchical visual cryptography for grayscale image 2016 [7]	Hierarchical Visual Cryptography Scheme Gray N Share Generation Algorithm	Applied only for monochromatic images, All shares are needed to retrieve secret image
Shubhangi Khaima, Reena Kharat [8]	Online Fraud Transaction prevention system using Extended Visual Cryptography and	Extended visual cryptography and QR code technique, random (2*2) matrix.	pixel expansion, complex approach

	QR code. 2016 [8]		
Fersna S, Athira V [9]	Progressive VCS Without Pixel Expansion For Color Images. 2015 [9]	Progressive Visual Cryptography Halftone	Pixel expansion

Naoki Kita, Kazunori Miyat et al in Magic sheets: Visual cryptography with common shares [2] an magic sheets approach is proposed to hide multiple images in sheets. The approach is based on (k, n) EVCS. Three share images along with 2 secret images is given as input in encryption process, so the secret images decrypted by combination of output shares. The quality of the decrypted resultant share optimization algorithm is proposed, but decryption process is consuming more time. The approach is demonstrated w.r.t (2, n) EVCS, but it has to be demonstrated using (k, n) EVCS. The approach suffers from pixel expansion and consuming more time to yield secret images. Most importantly information leakage is observed which has to be analyzed.

Yamini Ravella, Dr.Pallavi Chavan et al in Secret encryption using (2, 2) vcs scheme with DCT compression[3] a (2, 2) visual cryptography scheme is used to encrypt the images for share generation along with DCT technique used to reduce the size. DCT is used before as well as after share generation, for the comparative study. Loss of information occurs even if the quality of the image increases using DCT.

K. Shankar, P. Eswaran et al in RGB Based Multiple Share Creation in VCS with Aid of Elliptic Curve Cryptography[4] Red, Green, Blue Color component pixel values are extracted and represented as Matrix (P*Q). Using secret sharing scheme multiple shares w.r.t each color component is created and blocks are created by divided those shares. Then those blocks are encrypted using elliptical curve cryptography method. During decryption the reverse process is applied to get original image. The result shows that Mean square error has to be minimized and on attack the PSNR of secret image degrades 50% of the original image.

Trupti and Rohit et al in A New Technique for Color Share Generation using Visual Cryptography [5] visual cryptography is applied to color images to create color shares. During encryption the Red, Green and Blue component from secret image are extracted and to the R Component Gray Share generation algorithm is applied. Color shares are created by combining generated R gray share with B and G components. During decryption Blue and G components are extracted leaving the R grey Shares. The R component is extracted and combined with Blue and Green components to retrieve the secret image. With multiple folds security is increased.

R.M.Shiny, P.Jayalakshmi, A.Rajakrishnammal, T.Sivaprabha, Abirami.R et al in An efficient tagged visual cryptography for color Images [6] Floyd and Steinberg error diffusion scheme is used to generate halftone color images. The Red, green and blue base shares generated using traditional visual cryptography. With the help of tag pattern base shares are stamped using probabilistic VCS to yield tagged shares. This helps the participants to identify relevant shares and increase security. During decryption those generated tagged shares are folded along y-axis to get back the base shares, which are stacked to get secret image. The quality of secret image and tag image is poor with loss of information.

Trupti Patel, Rohit Srivastava et al in Hierarchical visual cryptography for grayscale image [7] an Hierarchical Visual Cryptography Scheme on gray image is proposed in which original image is encrypted in to N number of levels hence the security of original image is increased. The New proposed gray share generation algorithm is used for generation of n number of shares. Two shares called share a and share b which is encryption first phase. These two shares generate four shares in second stage of encryption and further successively shares are generated from each shares in third stage which is a chain process generating 8 shares. At decryption side if all 8 shares are stacked together to get original image but applicable only for gray images.

Shubhangi Khaima, Reena Kharat et al in Extended Visual Cryptography and QR code for Online Fraud Transaction prevention system [8] an extended visual cryptography technique is used to provide security during online Transaction against Phishing website. Considering QR code image of OTP, shares are created by generating a random matrix filled with 0 and 1based on the pixel values of the original image. Those shares are embedded in an cover image for advance security, but suffers from pixel expansion.

Fersna S, Athira V et al in Progressive VCS Without Pixel Expansion For Color Images [9] secret image is decomposed in to monochromatic images of Red, Green and blue tones. Using halftone technique these images are converted into binary image. The Zen-Yu and Chang Progressive VC method is used to create n shares for three monochromatic images and embedding process is carried out. During decryption shares of RGB channels are extracted which is gray scale and combined to get colored secret image.

Existing method performance is compared using Peak Signal to Noise Ratio value(PSNR). Table 1 and Figure 2 express PSNR value of few techniques conducted on Pepper image.

Table I: Comparison of VCS technique experimental PSNR values on Pepper image

Method	Experimental PSNR value of Pepper image
EVCS with Common Share, share optimization algorithm [1]	13.94
Elliptic Curve Cryptography as reported by Naoki Kita, Kazunori Miyat [3]	56.684
Progressive visual cryptography as reported by Fersna S, Athira V [9]	51.1427

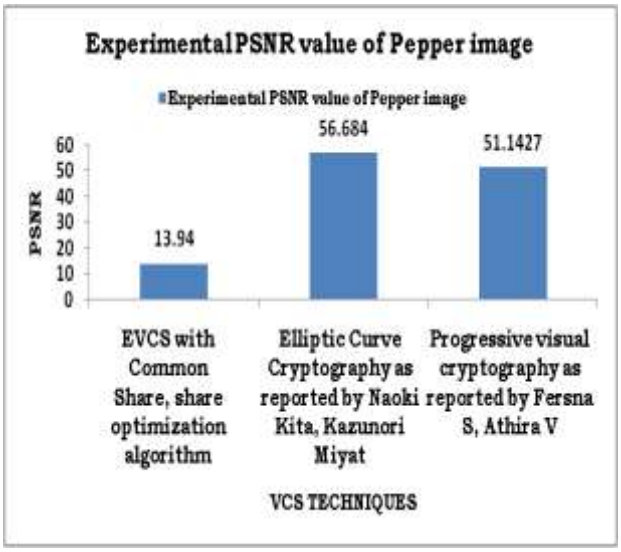

Figure 2: Comparitive analysis of VCS techniques using experimental PSNR value of pepper image

III. OVERVIEW ON STEGANOGRAPHY TECHNIQUES

Author Name	Title and Year	Method	Disadvantage/Problem
Nadeem Akhtar, Vasim Ahamad, Hira Javed [10]	A Compressed LSB Steganography Method 2017 [10]	LSB with modulo function.	cannot hide the secret data with fewer repetitions
Zaid and Ahmad [11]	Secure LSB Steganography for Colored Images Using Character-Color Mapping 2017 [11]	mapping Character and color range , color level modification along with pixel selection model	Well suited for text message , threshold value relays on message size, More Complex
Samaher Al-Janabi, Ibrahim Al-Shourbaji [12]	A Hybrid Image steganography method based on genetic algorithm 2017 [12]	Mixing matrix with Genetic Algorithm	Works with same size cover and secret image
Vinodhini, Malathi and Gireesh [13]	A Survey on Image Steganography Based on Least Significant Bit Matched Revisite (LSBMR) Algorithm 2016 [13]	Least Significant Bit Matched Revisited (LSBMR)	Not strong against visual attacks and pixels difference is not considered
Sabeen, Sajila and Bindiya [14]	A Two Stage Data Hiding Scheme with High Capacity Based on Interpolation and Difference Expansion Science Direct 2016 [14]	Enhanced Neighbor Mean Interpolation (ENMI) and Difference Expansion	Low PSNR value. Because of difference expansion in the second stage.
Nosrati, and Karimi [15]	Steganography in Image Segments Using Genetic Algorithm. 2015 [15]	Genetic Algorithm and LSB	Less Secure
Huang, and Jiwu [16]	Improved Algorithm of Edge Adaptive Image Steganography Based on LSB	Sobel edge detection and Edge based Adaptive Least Significant Bit Matching Revisited	Pixel pairs can be spotted by Brute force approach and works only on gray scale images

	Matching Revisited Algorithm 2014 [16]		
Khodaei and Faez [17]	New adaptive steganographic method using least significant-bit substitution and pixel-value differencing, 2012 [17]	LSB and PVD	Complexity in process ,low hiding capacity and PSNR
J. Chen, Chang and Le [18]	High Payload Steganography Mechanism Using Hybrid Edge Detector 2010 [18]	canny and fuzzy edges detection with LSB Substitution	Works for limited datasets. Not for 'Baboob' image

Nadeem Akhtar, Vasim Ahamad, Hira Javed et al in A Compressed LSB Steganography Method [10] an improved LSB Steganography method is proposed. The secret data is broken down into smaller components and embedded using modulo function in an cover imge. Where the image is divided into quotient and remainder sequence. The remainder sequence is embedded into cover image using a repetition loop based on quotient value. With the increase in number of repetition in secret data components better quality of stego image i.e better PSNR is achieved. The drawback of proposed method is that images with low repetition value cannot hide secret data like baboon, which cannot be embedded in Lena image because size of compressed groups is larger.

Zaid, Ahmad et al in Secure LSB Steganography for Colored Images Using Character-Color Mapping [11] a new algorithm is proposed for LSB-embedding method for color images. The pixels represent the message and LSB technique is used to conceal the message. A Dictionary that maps character to color range is shared among both sender and the receiver. In the proposed pixel selection model, based on message size a threshold value is set, which is used to select the pixels suitable for embedding the message. Pixels which differ from its adjacent pixels by a threshold value is selected for embedding. A binary search tree is constructed using pixel position so the order of pixel selection for embedding becomes easy. The pixel position as key value and message is embedded as cover image using RGB-color level modification steganography. Where During embedding a color channel is chosen and secret message is embedded using LSB technique. The proposed algorithm provides good Stego-image quality but embedding capacity per pixel has to be increased.

Samaher Al-Janabi, Ibrahim Al-Shourbaji et al in a Hybrid Image steganography method based on genetic algorithm[12], mixing matrix technique is used in steganography implementation and Genetic algorithm (GA) is used for optimizing mixing matrix creation by generating key and in the process of selecting optimum mixing matrix values. The cover image and secret image is transformed to one dimensional or 3D matrix from two dimensional based on the number of inputting images called Mixing matrix. Mixing matrix and matrix of mixed image is multiplied to generate stego image matrix

R E Vinodhini, P Malathi, et al in A Survey on Image Steganography Based on Least Significant Bit Matched Revisited (LSBMR)[13], pixels from cover image is used by LSBMR to conceal the secret information. The pixel 'x_i' stores secret message bit m_i and the pixel xi+1 stores mi+1 message bit and Consecutive Pixels concealing is achieved using LSBMR Embedding Process. Advantage is it's tough to find out the data hidden comparatively from LSB method so it can resist steganalaysis attacks such as RS-analysis. Disadvantage of LSBMR algorithm is it does not consider the difference among pair of pixels and it is suffers from visual attacks.

Sabeen Govind, Sajila, Bindiya Varghesec et al in A Two Stage Data Hiding Scheme with High Capacity Based on Interpolation and Difference Expansion Science Direct[14], an high embedding capacity two stage data hiding scheme is proposed in which Image interpolation is used to transform initial input image to high quality cover image, by using Enhanced Neighbor Mean Interpolation (ENMI) and in data embedding stage, pixel value difference between original and interpolated are considered. Which is then utilized for data embedding. The system gives enhanced payload capacity with an acceptable visual quality. Because of difference augmentation hitch in the second stage, resultant image suffers from low PSNR. This can be eliminated by some constant value, determined by the image characteristics.

Nosrati, H,anani and Karimi et al in Steganography in Image Segments Using Genetic algorithm[15] an Heuristic Genetic based message hiding technique is proposed. Gefore embedding data appropriate places in carrier image is spotted using Genetic Algorithm. The LSB of secret message and carrier image has to be extracted in an array in the format of strings of 0's and 1's and the secret image is embedded using LSB technique. On applying Genetic Algorithm blocks of image i.e segmentation is achieved and the address of blocks is stored in the key array which is used during extraction of secret message. The experimental results are better in visual quality of recovered image but message can be extracted using brute force technique.

Fangjun, Yane, and Huang et al in Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm[16] proposed an edge adaptive based LSBMB using Sobel's operator i.e sobel edge detection algorithm., which is used to detect the edges for embedding messages. The sharp edges are considered for embedding messages when the embedding rate is less. When the embedding rate is high less sharp edges are used for embedding purpose and the messages are embedded using LSB. The proposed method resists visual attacks but works only on gray scale images.

M. Khodaei, K. Faez et al in New adaptive steganographic method using least significant-bit substitution and pixel-value differencing, IET Image Process[17], non-overlapping blocks with 3 consecutive pixels in each block is created from cover image. The second pixel i.e. central pixel is called base pixel used to embed the information using LSB Technique and Optimal Pixel Adjustment process. Later PVD between the base and two other pixels in each block is calculated and then, modified PVD algorithm is applied to embed secret data in two pixels. The PSNR and Embedding capacity is good compared to other techniques.

Chen, Chang and T. H. N. Le et al in High Payload Steganography Mechanism Using Hybrid Edge Detector[18], an high hiding capacity achieved by LSB and hybrid edge detection scheme. Canny and fuzzy edges detection methods are applied for edge computation and the

LSB substitution method is used to embed hidden data. By proposed method data with higher PSNR is embedded with an LSB method. The method is tested with limited images dataset. The method is not tested using extensive edges based image like 'Baboob.tif.

Comparative analyses of existing methods are analyzed by Peak to Signal Ratio Value as shown in Table II and same is expressed in Figure 3.

Table II: comparison of steganography technique on Lena cover image of size 512 *512

Cover image Lena	
Methods	PSNR value using an cover image of size 512*512
Compressed LSB Steganography[10]	40.33
Secure LSB Steganography for Colored Images Using Character-Color Mapping [11]	52.33
Two Stage Data Hiding Scheme Based on Interpolation and Difference Expansion [14]	38.95
New adaptive steganographic method using least significant-bit substitution and pixel-value differencing [17]	37.63

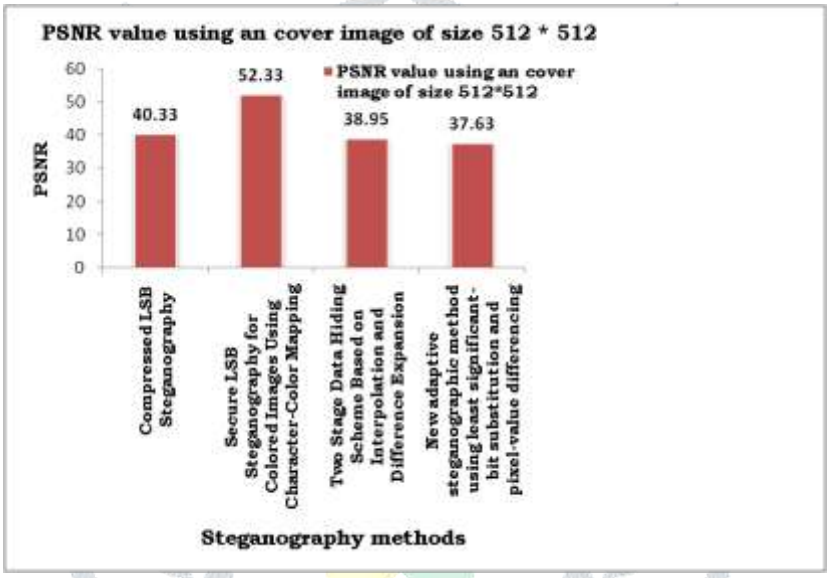

Figure 3: Comparative analysis of PSNR value of steganography techniques using cover image LENA

Thetemplateisusedtoformatyourpaperandstylethetext.Allmargins,columnwidths,linespaces,andtextfontsareprescribed;pleasedonotalterthem. Youmaynotepeculiarities.Forexample,theheadmargininthistemplatemeasuresproportionatelymorethaniscustomary.Thismeasurementandothersa redeliberate,usingspecificationsthatanticipateyourpaperasonepartoftheentireproceedings,andnotasanindependentdocument.Pleasedonotrevisean yofthecurrentdesignations.

IV. CONCLUDING REMARKS

In this paper a glimpse with the insight of the various cryptography and steganography techniques, their outcomes with respect to performance measures and their disadvantages are enumerated with respect to securing data are discussed. This paper also spotlights the existing work limitations and its merits. Pointing out open issues and techniques to be carried out leads us to come out with better performance measures in real time directs for Future Research.

REFERENCES

REFERENCES

[1] Deepesh Rawat and Vijaya Bhandari ,"*A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image",* International Journal of Computer Applications by IJCA Journal Volume 64 - Number 20 on 2013.

[2] 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.

[3] Yamini Ravella ; Pallavi Chavan, "*Secret encryption using (2, 2) visual cryptography scheme with DCT compression",* IEEE International Conference on Intelligent Computing and Control Systems (ICICCS) June 2017.

[4] K. Shankar and P. Eswaran, "*RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography",* IEEE China Communications journal, Volume: 14, Issue 2, February 2017.

[5] Trupti Patel and Rohit Srivastava, "*A new technique for color share generation using visual cryptography",* IEEE International Conference on Inventive Computation Technologies (ICICT), Aug. 2016.

[6] 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.

[7] Trupti Patel and Rohit Srivastava, *"Hierarchical visual cryptography for grayscale image",* IEEE Online International Conference on Green Engineering and Technologies (IC-GET) 2016.
[8] Shubhangi Khairnar and Reena Kharat , "*Online fraud transaction prevention system using extended visual cryptography and QR code",* IEEE International Conference on Computing Communication Control and automation (ICCUBEA) 2016.
[9] Fersna S and, Athira V, "*Progressive visual cryptography scheme without pixel expansion for color images"*, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 4, Issue 6, June 2015.
[10] Nadeem Akhtar , Vasim Ahamad and Hira Javed, "*A compressed LSB steganography method",* IEEE 3rd International Conference on Computational Intelligence & Communication Technology (CICT) Feb. 2017.//
[11] Zaid Y. Al-Omari and Ahmad T. Al-Taani, "*Secure LSB steganography for colored images using character-color mapping*", IEEE 8th International Conference on Information and Communication Systems (ICICS) April 2017.
[12] Samaher Al-Janabi and Ibrahim Al-Shourbaji, "*A Hybrid Image steganography method based on genetic algorithm*", IEEE 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) December 2017.
[13] G. L. Smitha and E. Baburaj, "*A survey on image steganography based on Least Significant bit Matched Revisited (LSBMR) algorithm*", IEEE International Conference on Emerging Technological Trends (ICETT) Oct. 2016.
[14] P.V. Sabeen Govind , M.K.Sajila and Bindiya M.V arghesea, "*A Two Stage Data Hiding Scheme with High Capacity Based on Interpolation and Difference Expansion*", International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST- 2015), Science Direct Procedia Technology journal, Volume 24, Pages 1311-1316, 2016.
[15] Masoud Nosrati, Ali Hanani and Ronak Karimi, "*Steganography in Image Segments Using Genetic Algorithm*", IEEE Fifth International Conference on Advanced Computing & Communication Technologies Feb. 2015.
[16] Fangjun Huang, Yane Zhong, and Jiwu Huang, "*Improved Algorithm of Edge Adaptive Image Steganography Based on LSB Matching Revisited Algorithm",* 12th International Workshop on Digital Watermarking , LNCS 8389 , pp. 19–31, 2014.
[17] M. Khodaei and K. Faez, "New adaptive steganographic method using least significant- bit substitution and pixel-value differencing", IEEE IET Image Processing journal , Volume: 6, Issue: 6, pages 677 - 686 , August 2012.
[18] Wen-JanChen, Chin-ChenChang and T. Hoang NganLe, "High payload steganography mechanism using hybrid edge detector", Science Direct Expert Systems with Applications Journal, Volume 37, Issue 4, Pages 3292-3301, April 2010.