ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review Paper on Data Hiding In 3D Barcode Image Using Steganography

Rama Rani
Research Scholar, Department of computer Engineering
Punjabi University, Patiala
Punjab, India

Gaurav Deep Sharma
Assistant professor, Department of computer Engineering
Punjabi University, Patiala
Punjab, India

Abstract: Steganography is an approach used to provide security to the confidential data in such a manner that only sender and receiver are able to use the data. In image steganography, image is used as a cover envelope to embed secret information. Today Barcodes system is very popular for protecting sensitive information. This paper introduces the concept of hiding data in 3D Barcode image using pattern generation approach. 3D Barcodes do not use any labels. They are embossed or engraved directly on the product during the manufacturing process.3D Barcodes use the same basic principal as 1D or 2D barcodes use. The performance evaluation is done by using statistical parameters.

Keywords: Steganography, Barcodes, data hiding, PSNR, MSE, Cover image, stego image.

INTRODUCTION TO STEGANOGRAPHY

With the tremendous development in modern digital technologies, the exchange of data and information becomes quite easy but at the same point concern related to the data confidentiality, integrity, security of information on the internet has become a major concern in today's modern era. [1]To accommodate the need for implementing security protocols on the data , a number of invisible and secret transmission approaches have been developed.to protect the data from several attacks , various information embedding techniques like cryptography, fingerprinting and steganography has been widely used. [1]

Secret concealing is one of the most acceptable technique to prevent the misplacement of fine data .The word "Steganography" has found in place from Greek Origin and means "covered writing" as it is composed of two words steganos means " covered" and graphy means " writing" .

Data can be embedded in any information carrier such as an image, audio, video, or text file. [2]

Cover channel + Hidden data + Secret Key = Stego channel

Generic Process of Steganography

In today's era, there are various approaches that are used to implement steganography but the general specification used in each approach is as follows:

<u>Concealed facts</u>: The facts or data that is to be transmitted over the network must not be known to the unauthorized person.

<u>Cover Channel</u>: The channel in which the sensitive information is to be concealed [1] <u>Stego key</u>: It is used for providing additional Security by implementing cryptography.

<u>Stego Channel:</u> This channel is same as the cover channel but it contains the sensitive information and it is sent over the network.

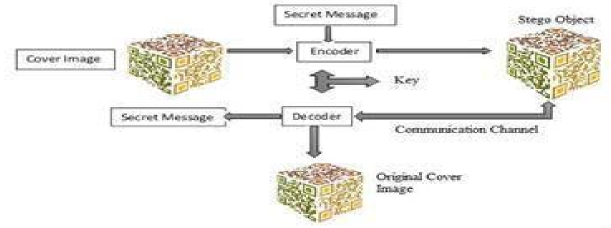


Figure 1 Basic model of steganography

A. Comparison of Steganography and Cryptography

In steganography we embed data in any cover medium in

S No	Feature	Steganography	Cryptography
1.	**Changing Information to a form unintelligible**	Yes	Yes
2.	**Concealing information**	Yes	No
3.	**Usage of Key**	Yes	Yes
4.	**Embedding the aspect of information**	Yes	No
5.	**Ensuring The anonymity of communication groups**	Yes	No
6.	**Amount of data to be transmitted**	Much greater the amount of information to encrypted	Comparable to the amount of encrypted information
7.	**Need Of extra Carrier**	Yes	No
8.	**Imperceptibility**	High	High
9.	**Applicability**	Universally Applicable	Universally Applicable
10.	**Technique**	Spatial Domain Frequency	RSA DSA Substitution
11.	**Robustness**	More Robust	Less Robust
12.	**Attacks**	Both detection extraction are difficult	Detection is easy but extraction is difficult

LITERATURE SURVEY

[1] A novel approach using modulo three strategy I used for embedding three secret images into a cover channel based on an improved least significant approach .In each gray pixel value it becomes possible to hide two ternary numbers. The proposed scheme results in the up gradation of quality of the image.

[2]In this paper author discusses techniques for hiding data In QR Codes. This paper explains various advantages and disadvantage of cryptography, fingerprinting, watermarking.

Various approaches are used to maintain the security of the data.

[3] In this paper a new technique called Integer Wavelet Transform (IWT) is utilized so it can reproduce the unique picture without any distortion. PIPA pre-processes host images by regulating the pixels into a definitive range for adequate reversibility. New watermark embedding is constructed by using SQH and clustering and extraction processes for good robustness and low run-time complexity. EPWM gives robustness for the robust and lossless watermark concealing and invisibility. Consequently this technique gives upgraded execution regarding, robustness, reversibility, limit and run-time complexity invisibility. It is promptly appropriate to various types of pictures.

[4] In this paper author described a new secure technique for hiding data in least significant bit images by making user of pattern generation of QR Code and LSB technique. This approach yields in better results as compared to the previous technique.

[5]With the evolution of internet Technology the need for the security of information during its transmission has also increased rapidly. A new framework for hiding data in image through least significant bit replacement is discussed. The Pixel Value difference of the region has also been taken into account in order to increase the embedding Capacity of data. A new fitness function has been designed for the Artificial Bee Colony Optimization Algorithm that helps to calculate the best positions where data can be embedded.

[6]In this paper, a brief discussion on steganography is done. The classification of steganography and the Methods used in image steganography is given in detail. A Comparison of the different image stenographic methods is done based on factors like embedding capacity and resistance to attacks .All the either vulnerable to attacks or their data hiding capacity is less.

[7]This paper emphasis on hiding numerous unrevealed imagesinanisolated24-bitcoverenvelopebyhidingdata in least significant bits through bit replacement approach. Each unrevealed dispatch is encoded before concealing in the cover envelope using transformation named Arnold.

Results indicate that the new framework efficiently secures the large payload information owing the visual level of communicated image adequately.

[8]The proposed methodology provides the feature that large amount of secret can be concealed into the boundary Regions rather than in the plane regions. This approach increase the quality of image and payload capacity by using two algorithms modified least significant bit approach and fuzzy approach. By using this approach it is easy to recognize boundary regions and plane regions more accurately. [9]This paper presents two layered security for data hiding by combining steganography and visual cryptography (VC).In this paper ,cover message and encrypted secret message are encoded into noise-like shares using(2,2)VC where concept of digital invisible ink of steganography is incorporated with VC(DIIVC) to hide secret message. Unlike typical steganography, shares are modified to conceal secret message instead of cover image .At receiver, decryption of shares using conventional VC results poor contrast cover image.

[10] It this paper, FT is used for concealing data in a cover medium. It is a frequency, Quick Response coded secret data is concealed in the Fresnelet coefficients of high frequency band. This technique results in an average peak signal to noise ratio of45.40dB and a concealing capacity of352, 332bits.Theseresultsprove the practical workability of the proposed technique for security.

[11] In This paper author introduces a new scheme called Edge adaptive scheme in which embedding regions are chosen based on the dissimilarity between two individual pixels and cover envelope size. For lesser concealing rates, only sharper boundary areas are used while keeping the other planar areas as they are. When the hiding amount Increases, more boundary areas can be rescued adaptively for data embedding by altering just a few measures.

[12]Communicating intimate information is an actual trial. Steganography deals with embedding confidential information in the image whereas cryptography is a bout modifying secret into a twisted form, so that it is blocked from intruder’s access. A secure data model is presented in this paper which uses steganography and cryptography. Quick Response codes are used for encrypting the encoded data.

[13]In this paper author presents a new technique for hiding data in an image. The used approach first converts plain text into chipper text and then hide the data into a cover media using SLSB method. This approach yields in better results than previous approaches.

[14]Steganography using ‘multimedia’ file (text, static image, audio and video).Steganalysis is a newly emerging Branch of data processing that seeks the identification of steganography covers, and if possible message extraction. It is similar to cryptanalysis in cryptography. The technique is ancient emerging monster that have gained immutable notice as it have newly penetrated the world of digital communication security. Objective is not only to prevent the message being read but also to hide its existence.

[15]This paper discusses subtractive clustering technique. To generate the initial centroid and uses partial contrast stretching to upgrade the quality of original channel. Image segmentation is the subdivision of an image into dissimilar sub images. In case of subtractive clustering centroid is generated by using the potential value of the centroid. So we use this approach to generate the initial centers and these centers are then used in k-means algorithm for the portioning of image. Then filtration is done to remove the useless portion of the image

[16]A new type of barcodes which have large data storage capacity called Quick Response barcodes became most popular. A new method for hiding datain2DBarcodes with greater data payload capacity. Formal information can be extracted from QR Code by making use of normal scanner but for extracting sensitive information, specialized scanner is required. The experiments reveal an adequate secret payload and the workability of the new scheme.

[17]This paper presents a novel image segmentation based Approach on DP clustering algorithm. The algorithm directly gives the no of the clusters of the image based on decision graph. Our proposed method could be an adequate preprocessing procedure for actions such as arrangement identification meaning evaluation.

[18]The supreme motive of this paper is to provide security at three stages, first is provided by making changes in the secret message, second by concealing complemented secret message in cover channel pixels that are selected randomly by making use of pseudorandom number generator and third

by using inverted bit LSB method 2 as stenographic technique rather than simple LSB, thus, lessen the possibility of the secret information being recognized. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements used to measure the difference between the cover-image and the stego-image.

CLASSIFICATION OF STEGANOGRAPHIC TECHNIQUES

There are different approaches used to classify Steganography techniques:

1. The first approach is to classify the Steganographic methods according to the type of cover channel used.

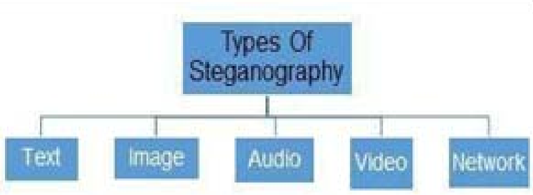


Figure2. Classification based on cover medium

2. The second approach is to classify the Steganography methods according to the modification performed on the embedding process in the cover medium.[14]

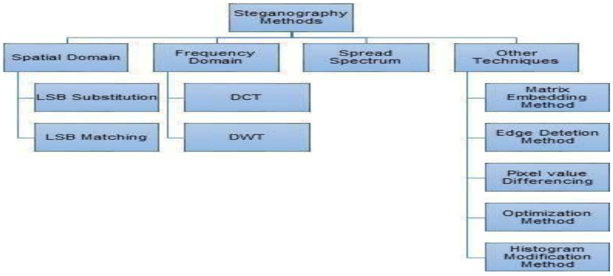


Figure4Classification of steganography methods

INTRODUCTION TO BARCODES

A barcode is a type of symbol which contains information related to an object. We can extract the information from barcode by making use of an optical Device. It is series of lines (usually black) on a light background (usually white). It simply represents data by using spaces. Barcodes are mainly categorized into three types. One Dimensional Barcodes (1D), Two Dimensional Barcodes (2D), Three Dimensional Barcodes (3D).

One Dimensional Barcodes: In one dimensional barcodes we can store information only in horizontal direction. We alsocall1Dbarcodes as linear barcodes. In these barcode numbers and letters are encoded in parallel lines. These type of barcodes are used everywhere such as in product transportation, business, medical industries .e.g. universal product code, code128.

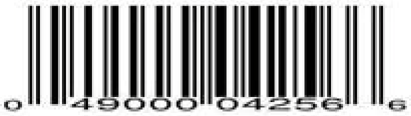


Figure5 One Dimensional Barcode

Two Dimensional barcode: In comparisonto1Dbarcodes 2Dbarcodesstorequietlargeinformation. We can store information in both vertical as well as horizontal direction.E.g.2DStackedBarcodes,2D Data Matrix barcodes.

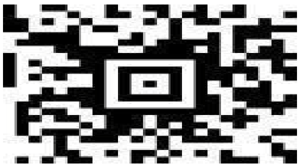


Figure6 Two Dimensional Barcode

Figure7Three Dimensional Barcodes

Three Dimensional Barcode: These barcodes use the same structure as 2Dbarcode. Theses barcodes use the third dimension for color. These barcodes has large data capacity than2Dbarcodes.Mostpopulartypeof3D barcode is PM Barcode.

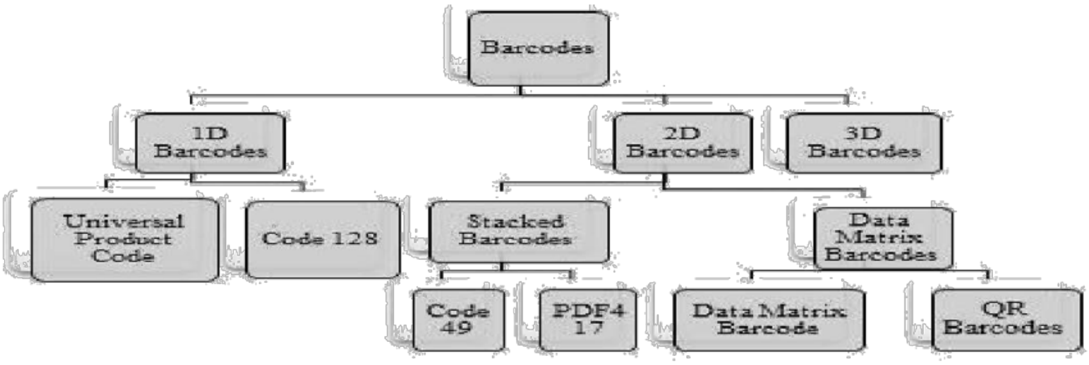
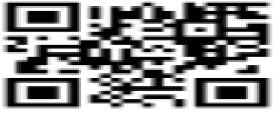


Figure8

A. Comparison of Barcodes

S. No	Parameter	1D Barcode	2D Barcode	3D Barcode
1.	Other name	It is called as One dimensional Barcode	It is called as two dimensional Barcode	It is called as three dimensional Barcode
2.	Pattern of data storing	It encodes numbers and letters	It stores data in two directions horizontal as well as vertical	These barcodes do not use any label. They are embossed or engraved during the manufacturing process.
3.	Data Storage capacity	Small	Big	Large
4.	Data Density	Low	Medium	High
5.	Correction function	No	Yes	Yes
6.	Information type	Number , English	Number , English , Picture	Number , English , Picture
7.	Durability	Less Durable	Durable	More Durable
8.	Advantage	It is less costly and extraction of data is easy	More reliable from security point of view. Can be read easily and write correctly.	Store large amount of data and can retain in high temperature.
9.	Disadvantage	It stores less amount of data i.e. up to 25 characters	These barcodes need special type of optical scanners to extract the information	Very costly
10.	Way of Scanning Data	Data is extracted based on the ratio of black to white	Date is read based based on black and white squares.	Data is read based on the height of the module.
11.	Example			

INTRODUCTION TO IMAGE PARTITIONING TECHNIQUES:

Image partitioning refers to partitioning an image into several regions acc. To some facts shared by pixels. Image partitioning is an elemental task and activity in computer sight and in image processing application. There are various approaches to partition an image. For image partitioning, Clustering is one of the most popular method. [15]

1. Thresholding
2. Clustering.
3. Edge or contour Extraction
4. Region Extraction.

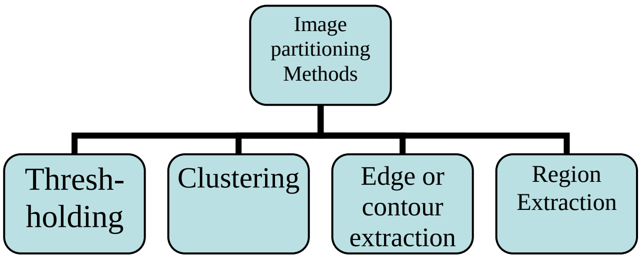


Figure9.ImagePartitioning Method

Thresholding: Thresholding techniques are based on finding the region of interest by separating foreground from background. Thresholding can be applied in three ways .Local methods are implemented based on local Features of pixel values and their neighborhoods. Global Methods separate region of interest by making use of Universal information (i.e.by using Texture features and histogram of image). Split, merge and growing methods are implemented based on geometric locations and similarity between pixel values in order to obtain better results of image.

Clustering: Clustering is defined as the procedure of clustering objects into groups whose data sets have similar characteristics. A cluster is thus an assembly of objects which are ‘alike ’between them and as ‘unalike’ to the objects belongs to other clusters.

Edge or contour detection: In an image an edge referred to as sudden change in pixel intensity value .Edges are detected to recognize the dissimilarities in an image. In this method of image partitioning, filters are used to remove the noise. Gradient in computed for detecting edges. There are several operators Robert, Sobel, Prewitt operators are used for identifying region of interest i.e. edges in an image.

Region Extraction: Region based segmentation is termed as resemblance based segmentation. Pixel values are Homologues to an object are grouped for image partitioning. The boundaries are recognized for image partitioning. Region includes only those pixels values that closely related to it. All the extracted regions contains pixel that have same intensity value. In region based image partitioning method the entire region R is partitioned into a number of regions [R1, R1, R2………..Rn]. These smaller regions when grouped form original image. There are various clustering methods.

1. K-Means clustering.
2. Fuzzy–Means clustering.
3. Progressive exponential K-means clustering
4. Iterative Partitioning Mean shift clustering.
5. Clustering based on density and distance.

Comparative study of Clustering Techniques

1. K-Means Clustering: This clustering is of unsupervised Type that partitions the input data into numerous classes on the basis of their inseparable distance from each other. The algorithm requires a color image as input. K is the number of clusters and a centroid will be assumed for each cluster. [15]

Advantages: Simple, understandable, Scalable. Efficient in large data set. Will always converge.

Disadvantages: Choosing K i.e. Optimal no .of clusters is difficult, Conjunction to local minima, Difficult to handle with noise and outliers.

2. Fuzzy-C Means clustering: One of the most powerful unsupervised approach is fuzzy c means clustering.

Sometimes data values on the border line between numerous classes do not completely belong to one of the class, but rather are assigned membership values in the Range 0 and 1 demonstrating their partial membership. FCM allows a data item to belong to two or more clusters.
Advantages: Unsupervised, Gives optimal results for overlapped data items.

Disadvantages: Large calculation time, Difficult to handle noise, more complex

3. Progressive Exponential K- Means clustering: This type of clustering technique is introduced to increase the data hiding capacity by reducing duplicacy. In this technique a color table is generated which includes all the colors of the real image. It involves three steps.
a).The generated color table is partitioned into a no. of groups using PEC algorithm.

b).The output contains a set of cluster C of various sizes, eachknowing2^ncolors, where n is cluster dependent size integer. Cluster area is increased by adding some other colors called virtual colors which are not present in original image. These colors Help in minimizing the distortion.

Advantages: Determining the similarity between two clusters always ensures that all the clusters are of equal sizes i.e. power of 2, Increased Payload capacity. Increased data security, Reduced concealing distortion.

Disadvantages: Complexity in handling with data values, large computational time.

4. Clustering based on density and distance: This Approach yields several advantages over existing techniques. By making use of decision graph, it directly indicates the no. of clusters to be used.

1. The centroids of the clusters can be easily and correctly determined.

   This technique uses two parameters.
   - Density
   - Distance

Advantages: Feasible de-noising approach for tasks such As pattern identification and image partition.
Disadvantages: Difficult to choose the value of

5. Iterative Partitioning Mean shift clustering: This clustering technique overcomes the disadvantages of conventional clustering algorithm. This algorithm uses number of iterations to segment or divide the image accurately with no. of selected clusters. It has three steps. 1. Preprocessing.
2. Color space modification.
3. Data item normalization.

Advantages: Improved technique performance, Less CPU Time, More Accuracy.

Disadvantages: Number of selected clusters are not optimal. Parameter based on the input image.

METHODOLOGY

There exists several approaches that can be used for embeddingsecretdatain3DBarcodeimages.3DBarcodes are usually represented by matrix. In the matrix we can store large amount of information. We are thus able to hide a large amount of information in barcodes. [10]

At Sender Side:

Step1: Overloading of information is of great concern in the secret embedding process. This happens only when the grayscale intensity value of the secret data pixel becomes greater than the low intensity value (0) or high intensity value (255).This overflow is controlled by filtering the cover image. There are a number of filters like high pass filters and low pass filters are used to filter the cover image.

Step2: The filtered image is then transformed into the colored image using HSI (hue, saturation, intensity) model. Step3.Inthisstepclustering is applied on the colored image. Clustering is a technique used to group the objects with similar properties.
Step4: Next, we have to recognize the largest cluster in which we can embed the secret message in an efficient

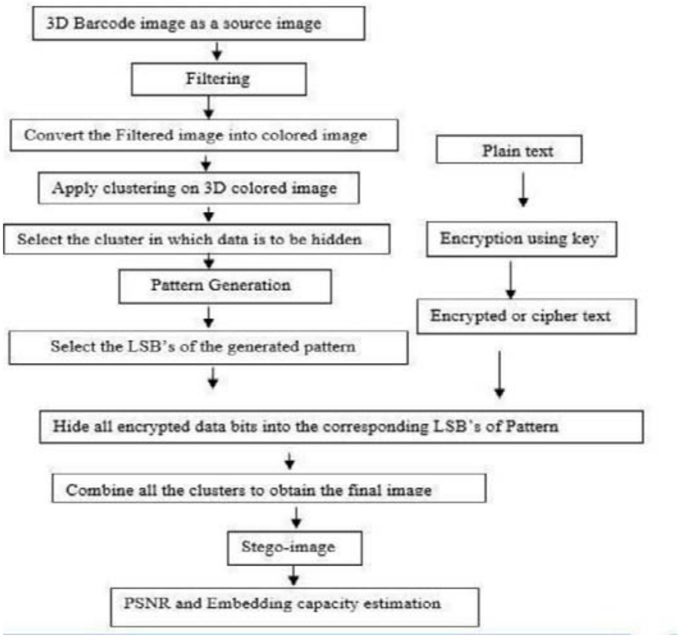
Way. The cluster can be selected on the basis of the size or Color.

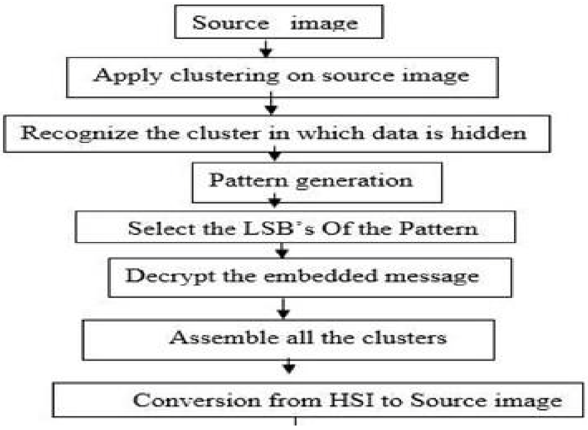
Step5: In this step the secret information is converted into encoded text by implementing cryptography by using Key. Step6: In this step a pattern is generated in the selected cluster. Pattern is generated in such a way that it can conceal the maximum data.

At Receiver Side:

The framework used at the receiver side includes following steps:

Step1.Thestegochannelgeneratedafterembedding the encoded information is taken as a source image.
Step2: Number of clusters of the stego image are created by applying clustering technique like using K-Means clustering.
Step3: Then we have to recognize the largest cluster in which the sensitive information or secret message is hidden.
Step4: After recognizing the cluster in which the data is hidden, we have to generate the pattern on the selected cluster in order to identify the least significant bits in which data is embedded.
Step5: In this step, by using the same key as used in the embedding phase we can decrypt the secret message.
Step6: All the clusters are the assembled.
Step7: Finally the HSI image is transformed back into the original image or cover image.


3D Barcode image as a source image
Filtering
Convert the Filtered image into colored image
Apply clustering on 3D colored image
Select the cluster in which data is to be hidden
Pattern Generation
Select the LSB's of the generated pattern
Plain text
Encryption using key
Encrypted or cipher text
Hide all encrypted data bits into the corresponding LSB's of Pattern
Combine all the clusters to obtain the final image
Stego-image
PSNR and Embedding capacity estimation


Source image
Apply clustering on source image
Recognize the cluster in which data is hidden
Pattern generation
Select the LSB's Of the Pattern
Decrypt the embedded message
Assemble all the clusters
Conversion from HSI to Source image

CONCLUSION

A new framework for concealing information into an image like 3D Barcodes is discussed in this paper. In this technique first of all a 3D barcode image is taken as input. As we all know in the data hiding process one of the major issue is the overflow of the data, this overflow is controlled by filtering the cover image using filters. Clusters are created based on the color pattern matching. The blue cluster with the largest number of pixels is selected to hide the data and a pattern is generated. The message to be concealed is encrypted using encryption technique and a pattern is generated. Then data is embedded into the least significant bits. The stego image is generated when embedding is completed. This technique proved to be more secure and effective as it cannot be easy to locate both the clusters and the pattern in which the secret message is concealed. The performance of the algorithm is evaluated by using statistical measures structure similarity index matrix, peak signal to noise ratio, Mean Square Error.

REFERENCES

[1] W. -L. Xu, C.-. C. Chang, T.-. S. Chen and L. -M. Wang,

[2] "An improved least-significant-bit substitution method using," ELSEVIER, 2016.

[3] M. RM and K. .N, "An Efficient Technique for Data Hiding with use of QR," International Journal of Computer Applications, vol. 100, no. 14, 2014.

[4] G. K. Reddy and A. V. Bhasha, "Robust Lossless Data Hiding Using Clustering And Statistical Quantity Histogram," JIRT, vol. 1, no. 8, 2014.

[5] D. A. . P. Kumar, M. Baskaran, J. Jocin and M. G. D. Daniel, "Data Hiding Using LSB with QR Code Data," IJSTE - International Journal of Science Technology & Engineering, vol. 2, no. 10, 2016.

[6] kaur, R. kaur and N. kaur, "Image Steganography using Discrete Wavelet," in 1st International Conference on Next Generation Computing Technologies (NGCT-2015), 2015.

[7] P. Joseph and V. S. , "A Study on Steganographic Techniques," in Proceedings of 2015 Global Conference on Communication Technologies(GCCT 2015), 2015.

[8] P. Das, S. . C. Kushwaha and M. Chakraborty, "MULTIPLE EMBEDDING SECRET KEY IMAGE," IEEE SPONSORED 2ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEM, 2015.

[9] H. Dadgostar and F. Afsari, "Image steganography based on interval-valued," ELSEVIER, 2016.

[10] Y. K. Meghrajani and H. . S. Mazumdar, "Hiding Secret

[11] Message using Visual Cryptography in," IEEE, 2015.

[12] S. U. Maheswari, and D. J. Hemanth, "Frequency domain QR code based image steganography usingFresnelet transform," International Journal of Electronics and, 2014.

[13] W. Luo, F. Huang and J. Huang, "Edge Adaptive Image Steganography Based on LSB," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 5, no. 2, 2010.

[14] Karthikeyan , A. . C. Kosaraju and S. . G. S, "Enhanced Security in Steganography using," IEEE, 2016.

[15] K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend," in 2015 Third International Conference on Image Infonnation Processing, 2015.

[16] R. Doshi, P. Jain and L. Gupta, "Steganography and Its Applications in Security," International Journal of Modern Engineering Research (IJMER), vol. 9, no. 2.

[17] N. Dhanachandra, K. Manglem and Y. J. Chanu, "Image Segmentation using K-means Clustering Algorithm and," in Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), 2015.

[18] W. -Y. Chen and J. -W. Wang, "Nested image steganography scheme using," Optical Engineering, 2009.

[19] Z. Chen, Z. Qi, F. Meng, L. Cui and Y. Shi, "Image Segmentation via Improving Clustering Algorithms with Density and Distance," ELSEVIER, 2015.

[20] R. Bhardwaj and V. Sharmab, "Image Steganography Based on Complemented Message and Inverted bit LSB," in 6th International Conference On Advances In Computing & Communications, 2016,.