IARJSET
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

An Improved Steganography Technique using Genetic Algorithm and Encryption Approach

Gagandeep Kaur[1], Baldip Kaur[2]

Student, LLRIET, Moga[1]

Assistant Professor, LLRIET, Moga[2]

Abstract: Image steganography is the process of data hiding so that information can be transmitted in secure manner. In the process of data hiding various approaches had been used for data embedding. In this paper a novel approach has been proposed so that data can be easily embedded behind the cover pixels. In the process of data hiding data integrity and confidentiality are major concerns that must be accumulated. In proposed work encryption approach has been used so that data security from various attacks can be achieved. In the proposed work multiple bits have been used for embedding of encrypted information. Performance metrics has been analyzed for validation of proposed system. On the basis of these parameters one can conclude that proposed approach provide better results as compare to existing one.

Keywords: Blow-Fish, Genetic Algorithm, LSB, MLSB and 4LSB

1. INTRODUCTION

1.1 Stegnography

Steganography is gotten from the Greek words "segos" signifying "spread" and "raffia" signifying composition characterizing it as "secured written work". In picture Steganography the data is shrouded only in pictures. The thought and practice of concealing data has a long history. In Histories the Greek history specialist Herodotus composes of an aristocrat, Hostages, who expected to speak with his child in-law in Greece. He shaved the leader of one of his most trusted slaves and tattooed the message onto the slave's scalp. At the point when the slave's hair developed back the slave was dispatched with the shrouded message. In the Second World War the Microdot system was produced by the Germans.

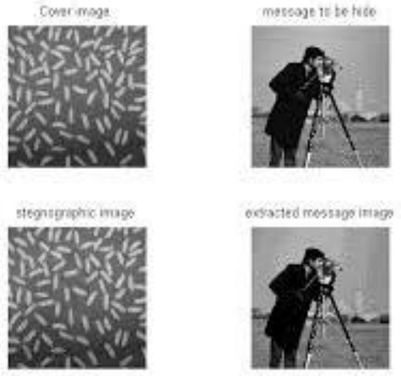


Figure1. Steganography

1.2 Uses of Steganography

- Steganography can be an answer which makes it conceivable to send news and data without being controlled and without the apprehension of the messages being blocked and followed back to us.
- It is additionally conceivable to just utilize steganography to store data on an area. Case in point, a few data sources like our private keeping money data, some military privileged insights, can be put away in a spread source. When we are obliged to unhide the mystery data in our spread source, we can undoubtedly uncover our saving money information and it will be difficult to demonstrate the presence of the military mysteries.
- Steganography can likewise be utilized to execute watermarking. Despite the fact that the idea of watermarking is not so much steganography, there are a few steganographic systems that are being utilized to store watermarks in information. The fundamental contrast is on aim, while the reason for steganography is concealing data, watermarking is just broadening the spread source with additional data. Since individuals won't acknowledge detectable changes in pictures, sound or feature records on account of a watermark, steganography systems can be utilized to conceal this.

DOI 10.17148/IARJSET.2018.5613

- E-business takes into consideration an intriguing utilization of steganography. In current e-business exchanges, most clients are ensured by a username and secret word, with no genuine technique for confirming that the client is the genuine card holder. Biometric unique finger impression filtering, joined with extraordinary session IDs inserted into the unique mark pictures by means of steganography, take into consideration an exceptionally secure choice to open ecommerce exchange check.
- Matched with existing specialized systems, steganography can be utilized to do concealed trades. Governments are keen on two sorts of concealed interchanges: those that help national security and those that don't. Computerized steganography gives incomprehensible potential for both sorts. Organizations may have comparative concerns with respect to insider facts or new item data.
- The transportation of delicate information is an alternate key utilization of steganography. A potential issue with cryptography is that meddlers know they have a scrambled message when they see one. Steganography permits to transport of delicate information past meddlers without them knowing any touchy information has passed them. The thought of utilizing steganography as a part of information transportation can be connected to pretty much any information transportation strategy, from E-Mail to pictures on Internet site.

1.3 Different Types of Steganography

1.3.1 Text stenography: Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data

1.3.2 Audio stenography: Audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

1.3.3 Protocol Steganography: The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.

1.3.4 Video Steganography: Video Steganography is a method to conceal any sort of records into convey Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file. This venture is the application created to insert any sort of data (File) in an alternate document, which is called transporter record. The bearer document must be a feature record. It is concerned with inserting data

1.4 Applications of Steganography

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several stenographic techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, Steganography methods can be used to hide this.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.
- It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.
- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification
- The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

2. LITERATURE REVIEW

Khan S et al. (2016) “Analysis of Data hiding in R, G and B Channels of Color Image using Various Number of LSBs” In today’s world of fast communication, to insure the security and integrity of information is a big challenge. Data hiding also known as Steganography is one of the fields that deal in methods related information security and hide secret information and message other information. This paper elucidates the effect of data hiding in different number of least significant bits in the primary colors of RGB color image. These individual color channels are analyzed at different hiding capacity level and its has been observed that high quality Stego images with PNSR 30dB and above can been obtained by hiding secret information in 5 least significant bits of red, green and blue channels, specially the green and blue channels give a very high visual quality. The individual channels can hide 20% data, i.e. one fifth of the overall size of cover image, with undetectable changes in cover image.
Joshi et al. (2016) “New Approach toward Data Hiding Using XOR for Image Steganography” with the growth in internet usage, there is proportional growth in security and privacy demands. In this paper, a three bit XOR steganography system for concealing messages into gray Images is projected. In this method, last three bits of pixel value offer 100 percentage of message addition. This new technique uses the XOR operation between the message and original image. If the intruder extracts the last three bits, he would not be able to find the meaning of the message as the message is in decoded form. The maximum no of bit which is to be hidden using this method is equal to the R*C*3, where R and C is the rows and column of the image. The time complexity Is also calculated which is equal to O(1). Later on the method is analyzed on the bases of PSNR, MSE, L2RAT and MAXERR. The projected technique is also matched with other similar techniques to show the superiority.
Behera et al. (2010) “Color Guided Color Image Steganography” Author want to propose that most of the data hiding methods in image Steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each pixel is replaced to hide bits of the secret message. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits. The hidden information can easily be uncovered using many known statistical steganalysis techniques, such as the X2 that can detect the concealed data inside the image with its original size.
Mahmoud Anke et al. (2010) “Pixel Indicator High Capacity Technique for RGB Image Based Steganography” in this paper author want to say that the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G green) and z-axis can be for B (blue).
Gutub et al. (2010) “Pixel Indicator Technique for RGB Image Steganography” in sequence, if the first indicator selection is the Red channel in the pixel, the Green is channel 1 and the Blue is the channel 2 i.e. the sequence is RGB. In the second pixel if we select, Green as the indicator, then Red is channel 1 and Blue is channel 2 i.e. the sequence is GRB. If in third pixel Blue is the indicator, then Red is channel 1 and Green is channel 2. The sequence of the algorithm is given below. The first 8 bytes at the beginning of the image are used to store the size of the hidden message, which is also used to define the beginning of the indicator channel sequence. These 8 bytes consumes all LSBs of the RGB channels, assuming it is enough to store the size of the hidden bits. To choose the first indicator channel, the size stored in the first 8 bytes is used. The indicator choice is assumed as the first level, followed by the data hiding channels as second level. All six possible selections are obtained from the length of message (N), which will control the sequence.

3. PROPOSED METHODOLOGY

Steganography is the field that deals with hiding of secret information behind cover object, so that data can be transmitted from source to destination in a secure manner. In the process of steganography a cover object has been selected for hiding of secret information behind the cover object. In the processing of extraction of information from cover object the receiver must know to the method of extraction of hidden information. In the process of steganography various approaches have been used for embedding of secret information. These approaches divides cover object into different bands and embedded secret information behind these parts of cover object.

3.1 Cover and secret Information

In the purposed work image steganography has been done for embedding of secret information behind pixels of image file. In this process image has been used as a cover object. In the process of image steganography different color regions of particular image has been extracted to embedding secret information. In the purposed work image has been used for embedding of secret information behind all the color regions of a single image file. Secret information that has to be embedded behind the cover image must be smaller in size as compare to cover image.

3.2 Data Encryption

In proposed work data encryption has been used so that data can be encrypted using blowfish approach. On the basis of

DOI 10.17148/IARJSET.2018.5613

blowfish approach secret key has been embedded to the secret information so that information can be converted to cipher text. Cipher text is the form of secret data that is in encoded format so that authenticated user can decrypted information through private key.

3.3 Data Embedding

After selection of cover and secret media cover image has been divided into different true color images that are red, green and blue images. After this process GA has been implemented on the image that provide information about the region available in the image that has minimum information variation and that can be easily changed through embedding of secret data. Multiple bits from the cover image regions have been extracted and used for data embedding.

3.4 Work flow of Embedding

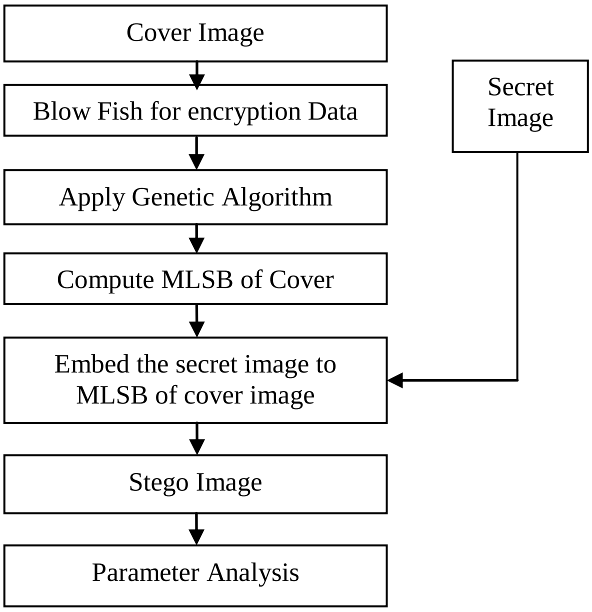


Figure2. Flow of proposed work for data embedding

3.5 Work flow of Extraction

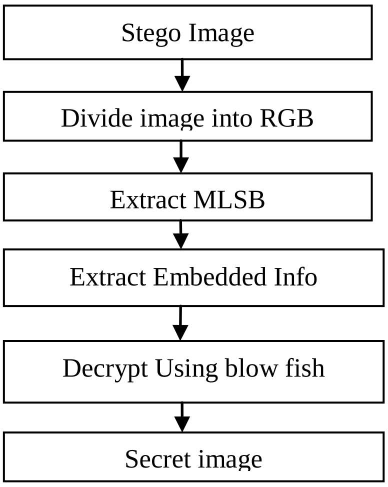


Figure3. Flow of proposed work for data Extraction

The above defined images have been used for representation of flow of the proposed work. In this process data has been used for data embedding behind the cover image. Figure 1 and figure 2 represents data embedding and data extraction process so that by using these steps data can be embedded and extracted from images.

3.6 Parameter Analysis

Various parameters have been analyzed for performance evaluation that has been explained below.

i) PSNR

PSNR stands for peak signal to noise ratio. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of the logarithmic decimal scale. PSNR is used to measure the quality of image (stego-image). The signal or input in this case is the original data, and the noise is the error introduced by compression. The PSNR is defined as:

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}_1^2}{\mathrm{MSE}}\right) \quad \ldots\ldots\ldots (1.1)$$

ii) MSE

Mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. It is basically a difference between the cover image and stego image. If the value of MSE is low, then the quality of the stego image is better. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator. The MSE is defined as:

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 .(1.2)$$

iii) SSIM

SSIM consists of three components: structure (loss of cor-relation), luminance (mean distortion) and contrast (variance distortion). In CT-IQA, the outputs of Content Detection and Texture Compensation provide a “reference image” (the difference image) and the quality of the “reference image”. The luminance and the contrast of an input image together determine the contribution of the input image to the “reference image”. We construct a specific example of a SSIM quality measure from the perspective of image formation. A previous instantiation of this approach was made and promising results on simple tests were achieved. In this paper, we generalize this algorithm, and provide a more extensive set of validation results.

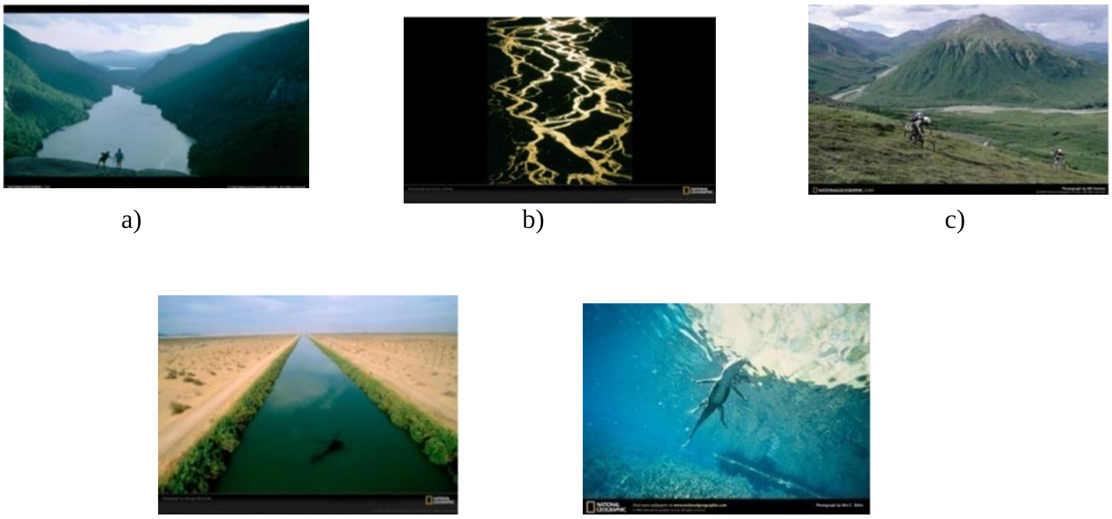
iv) CORRELATION

Correlation is a statistical measure of image security that expresses a degree of relationship between two adjacent pixels in an image. In most of the natural images, the values of neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). The aim of correlation measure is to keep the amount of redundant information available in the encrypted image as low as possible.

4. EXPERIMENTAL RESULTS

The proposed work has been implemented using MATLAB 2012b.For evaluation of proposed work five images have been used named Lake.jpg, Art.jpj, Mountain.jpg, River.jpj and Sea.jpg as mentioned in figure

Figure4. Cover Image



a) b) c)

d) e)

Figure5. Images used for evaluation

4.1 Evaluation of proposed work

We are using different images for the evaluation of the proposed work and do comparision on the basis of different parameters.

4.1.1 PSNR

PSNR stands for peak signal to noise ratio. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of the logarithmic decimal scale. PSNR is used to measure the quality of image (stego-image).

Table 4.1 Parameters on the basis of PSNR

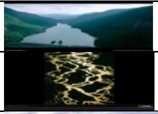
Image	Images	MLSB	4LSB
Lake.jpg		78.90	70.69
Art.jpg		75.69	71.40
Mountain.jpg		77.98	80.56
River.jpg		79.78	87.45
Sea.jpg		80.48	77.56

Table 4.1 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter PSNR has been evaluated for different images and values has been represented in tabular form for proposed and existing technique.

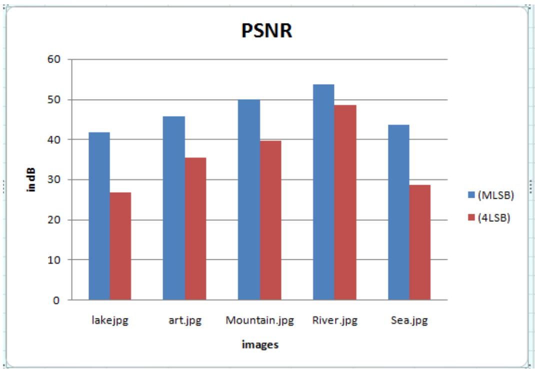


Figure6. Comparison graph of proposed work with exiting using PSNR

Fig. 3 represents graphical representation of performance evaluation parameter correlation with existing approach. As graph represents proposed wok provide better PSNR than existing approach.

4.1.2 MSE

Mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. It is basically a difference between the cover image and stego image. If the value of MSE is low, then the quality of the stego image is better.

Table 4.2 Parameters on the basis of MSE

Image	Images	MLSB	4LSB
Lake.jpg		6.58	10.69
Art.jpg		2.36	9.24
River.jpg		5.69	15.36
Mountain.jpg		3.59	8.69
Sea.jpg		4.36	9.38

Table 4.2 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter MSE has been evaluated for different images and values has been represented in tabular form for proposed and existing technique.

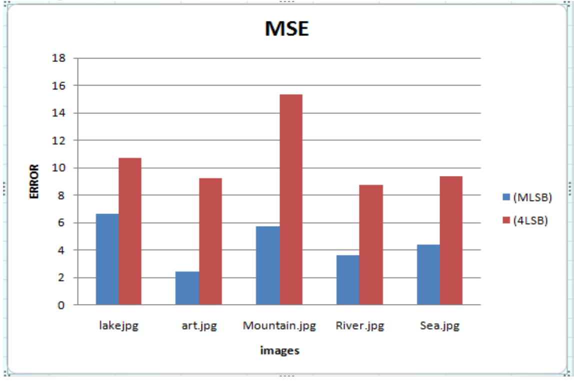


Figure7. Comparison graph of proposed work with exiting using MSE

Figure7. Represent graphical representation of performance evaluation parameter MSE with existing approach. As graph represents proposed work provide less mean square error than existing approach.

4.1.3 SSIM

SSIM consists of three components: structure (loss of cor-relation), luminance (mean distortion) and contrast (variance distortion). In CT-IQA, the outputs of Content Detection and Texture Compensation provide a “reference image” (the difference image) and the quality of the “reference image”. The luminance and the contrast of an input image together determine the contribution of the input image to the “reference image”. We construct a specific example of a SSIM quality measure from the perspective of image formation.

Table 4.3 Parameters on the basis of SSIM

Image	Images	MLSB	4LSB
Lake.jpg		0.92	0.87
Art.jpg		0.95	0.89
Mountain.jpg		0.98	0.93
River.jpg		0.91	0.81
Sea.jpg		0.96	0.90

Table 4.3 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter SSIM has been evaluated for different images and values has been represented in tabular form for proposed and existing technique

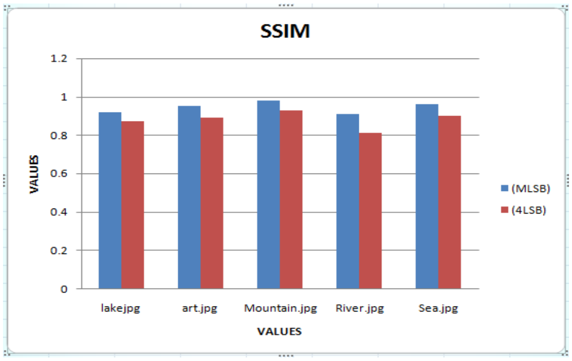


Figure8. Comparison graph of proposed work with exiting using SSIM

Figure8. Represent graphical representation of performance evaluation parameter SSIM with existing approach. As graph represents proposed wok provide better SSIM than existing approach.

4.1.4 CORRELATION

Correlation is a statistical measure of image security that expresses a degree of relationship between two adjacent pixels in an image. In most of the natural images, the values of neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). The aim of correlation measure is to keep the amount of redundant information available in the encrypted image as low as possible.

Table 4.4 Parameters on the basis of Correlation

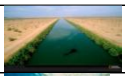
Image	Images	MLSB	4LSB
Lake.jpg		0.99	0.91
Art.jpg		0.98	0.93
Mountain.jpg		0.99	0.92
River.jpg		0.99	0.92
Sea.jpg		0.97	0.90

Table 4.4 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. The parameter Co-relation has been evaluated for different images and values has been represented in tabular form for proposed and existing technique.

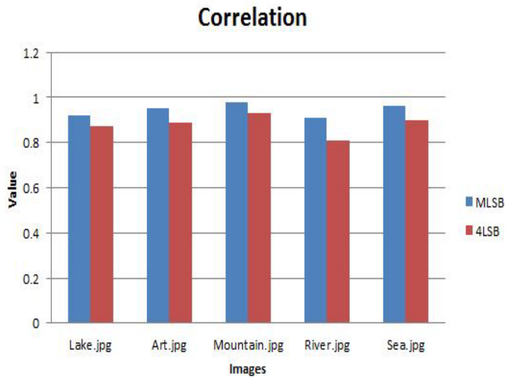


Figure9. Comparison graph of proposed work with exiting using Correlation

Figure9. Represent graphical representation of performance evaluation parameter correlation with existing approach. As graph represents proposed wok provide better correlation than existing approach.

5 .CONCLUSION AND FUTURE SCOPE

In the proposed work image steganography has been used so that data can be easily embedded behind the cover image with minimum distortion in cover media. In the proposed work hybrid approach of image steganography and data encryption has been proposed. In this process secret information that has to be transmitted has been encrypted using encryption approach. Encryption approach converts the originality of the information in cipher text. This cipher text has been embedded behind the cover image so that data can be transmitted in secure manner. In this process of data embedding image has been divided into RGB spectrum and the fuzzy set of rules have been implemented on the image so that region from the image can be extracted that can be used for data embedding in efficient manner. In this process the multiple least significant bits have been extracted from the red, green and blue region of the image. These least significant bits have been used for embedding of secret information that has been encrypted. Whole information has been embedded to the least significant bits and the all the color bands have been restored to obtain a single stego image that contains secret information. In the future reference proposed approach can be used in real world application for data security and transmission. In the future new approaches that are based on artificial intelligence that can be used for images steganography so that regions from the images can be extracted in which data can be embedded at high capacity with minimum distortion

REFERENCES

[1] Sahib Khan, “Analysis of Data hiding in R, G and B Channels of Color Image using Various Number of LSBs”, IEEE Conf. on Color image, 2016, pp 34-45.

[2] Kamaldeep Joshi “New Approach toward Data Hiding Using XOR for Image Steganography”, IEEE Conf. on XOR, 2016, pp 129-137.

[3] Getup, A. “Pixel Indicator Technique for RGB Image Steganography”, Journal of Emerging Technologies in Web Intelligence, Vol. 2, No.1,IEEE,2010, pp. 193-198.

[4] P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," 2010 Second International conference on Computing, Communication and Networking Technologies, Karur, 2010, pp. 1-6.

[5] Bailey, K. “An evaluation of image based Steganography methods”, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, IEEE, 2006, pp. 55-88.

[6] Mahata, S.K. “A Novel Approach of Steganography using Hill Cipher”, International Conference on Computing, Communication and Sensor Network (CCSN), IEEE, 2012, pp. 0975-888.

[7] Chapman, M. Davida G, and Rennhard M. “A Practical and Effective Approach to Large Scale Automated Linguistic Steganography” found online at http://www.nicetext.com/doc/isc01.pdf.

[8] Mehboob, B. “A Steganography implementation”, Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium, ISSN 978-1-4244-2427-6, IEEE, 2008, pp.1–5.

[9] Marwaha, P. “Visual cryptographic Steganography in images”, Second International conference on Computing, Communication and Networking Technologies**,** IEEE, 2010, pp. 34-39.

[10] Mahata, S.K. “A Novel Approach of Steganography using Hill Cipher”, International Conference on Computing, Communication and Sensor Network (CCSN), IEEE, 2012, pp. 0975-888.

[11] Saravanan, V, Neeraja, A. “Security issues in computer networks and steganography”, IEEE 7th International Conference on Intelligent Systems and Control, pp. 363-366, 2013.

[12] Shaikh Shakeela ; P. Arulmozhivarman ; Rohit Chudiwal ; Samadrita Pal “Double coding mechanism for robust audio data hiding in videos” Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, pp 34-45.

[13] K. Saranya ; R.S. Reminaa ; S. Subhitsha “Modern applications of QR-Code for security” Engineering and Technology (ICETECH), 2016, pp 34-40.

[14] Dhiraj D. Shirbhate ; S. R. Gupta “Digital forensic techniques for finding the hidden database using analytical strategies” Information Processing (ICIP), 2015 , pp 221-227.

[15] Jas R Sheth “Snake and ladder based algorithm for steganographic application of specific streamline bits on prime gap method” Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014, 10-11 July 2014.

[16] Ammad Ul Islam ; Faiza Khalid ; Mohsin Shah “An improved image steganography technique based on MSB using bit differencing” Innovative Computing Technology (INTECH), 24-26 Aug. 2016.

[17] Vineeta Singh ; Priyanka Dahiya ; Sanjay Singh “Smart card based password authentication and user anonymity scheme using ECC and steganography” Advances in Computing, Communications and Informatics (ICACCI, 2014 , pp 29-34.

DOI 10.17148/IARJSET.2018.5613