

Improve Image Steganography using Random Password Generation for Secure Transmission of Data

Sukhjinder Pal Kaur
Research Scholar
Department of CSE
SBS State Technical Campus, Ferozepur

Sonika Jindal
Assistant Professor
Department of CSE
SBS State Technical Campus, Ferozepur

ABSTRACT

Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. LSB technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this process image is divided into different regions for the detection of least significant bits available in different images. Image pixel available in the image is a combination of three different colours red, green and blue. Modifications over traditional LSB method are introduced to increase the amount of data that can be hidden in the cover image. In addition, to increase data protection our algorithm have a built in encryption technique. As LSB the output image of algorithm will look identical to the cover image.

Keywords

LSB & ISB, Image, Security, Steganography, PSNR, MSE

1. INTRODUCTION

1.1 Steganography

The Steganography, cryptography & digital watermarking technique is used to give security of data. Steganography, is a type of hiding data inside another data like cover medium by applying techniques of Steganography. Cryptography & digital watermarking make data human unreadable called cipher thus cryptography is scrambling of message. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography.

1.2 Uses of Steganography

- Steganography is an answer which makes it conceivable to send news & data without being controlled & without being controlled & without the apprehension of message being blocked back to us.
- 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 added to conceivable to just utilize steganography to hide data on an particular area.
- 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 inside.
- Steganography is use to execute watermarking. This idea is not too much steganography. There are some

steganography systems that are utilized to store watermark. 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.

- 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.
- With existing specialized system, steganography is used to concealed trades. Govt are keen on two sort of concealed interchange. 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 sites.

1.3 Different kind of Steganography

Various types of steganography approaches are available that has been used for hiding data behind various cover medias. These types of steganography have been illustrated under described sections.

1.3.1 Text Steganography

Hiding data in content is the most vital strategy for steganography. The method was to hide a misery message in every nth letter of each expression of an instant message. In the wake of blasting of Internet and diverse kind of advanced document groups it has diminished in importance. Content Steganography utilizing computerized records is not utilized frequently in light of the fact that the content documents have a little measure of repetitive information.

1.3.2 Audio Steganography

Audio steganography is used to misuses the properties of the human ear to shroud data unnoticeably. A perceptible, sound can be imperceptible in the surrounding area of an alternate

louder audible sound. This property permits to choose the divert in which to shroud data.

1.3.3 Image Steganography

Image is utilized as the prominent spread items for steganography. A message is implanted in a computerized picture through an implanting calculation, utilizing the mystery key. The resulting stego picture is send to the receiver. On the other side, it is handled by the extraction calculation utilizing the same key. During the transmission of steno picture unauthenticated persons can just recognize the transmission of a picture however can't figure the presence of the concealed message.

1.3.4 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.

1.3.5 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. The least significant bit (LSB) insertion is an essential methodology for implanting data in a transporter record. Least significant bit (LSB) insertion system works on LSB bit of the media document to conceal the data bit.

2. REVIEW OF LITERATURE

Yang Ren-er et al [1]: “Image Steganography Combined with DES Encryption Pre-processing” With a particular ultimate objective to upgrade the security of steganography, this paper thought about picture steganography joined with preprocessing of DES encryption. Exactly when transmitting the riddle information, firstly, encode the information anticipated that would conceal by DES encryption is mixed, and a short time later is formed in the photo through the LSB steganography. Encryption estimation improves the minimum coordinating execution between the photo and the puzzle information by changing the quantifiable traits of the riddle information to update the resistance to acknowledgment of the photo steganography. The trial comes about showed that the resistance to recognizable proof quality of picture steganography joined with preprocessing of DES encryption is found much well than the way using LSB steganography computations clearly.

Guo, J.-M et al [2]: “Quality Compressed Steganography Using Hidden Referenced Half toning” Piece truncation coding is a beneficial pressing framework while offering incredible picture quality. In any case, the blocking sway inherent in BTC causes extraordinary perceptual antiquated irregularity in high weight degree applications. In this paper, a blunder diffused piece truncation coding (EDBTC) is proposed to deal with this issue. As demonstrated by the EDBTC, the slip by achieved by the refinement between the principal grayscale pixel regard and the correspondingly high or low mean substitute is diffused to the predefined neighborhood, and in this manner the typical grayscale will be taken care of ceaselessly. The SSS has the limit flow message into various host pictures and in this manner upgrades the security. The CES has the limit pass on secure message by method for shading introduced CSHRH picture. Both expansions are in like manner with an extra benefit of achieving high farthest point message convection.

Mathkour, H et al [3]: “A New Image Steganography Technique” Different picture steganography strategies have been proposed. In this paper, we examine various steganography methods and devices. We express a set of criteria to dissect and assess the qualities and shortcomings of the displayed strategies. We propose a more vigorous steganography procedure that takes preferences of the qualities and maintains a strategic distance from the constraints.

Bandyopadhyay, S.K. et al [4]: “Network Based Public Key Method for Steganography” Steganography (a brutal Greek translation of the term Steganography is puzzle composed work) has been used as a piece of various structures for quite a while. It has found use in diversely in military, political, individual and authorized advancement applications. Immediately communicated, steganography is the term associated with any number of methodology that will cover a message inside an article, where the disguised message won't be evident to a spectator. The main steganography applications used “invalid figures”, or clear substance. An invalid figure passes on that the message has not been encoded by any stretch of the imagination, whether it is using fundamental character moving, substitution or impelled propelled encryption estimation. In this way, the message is routinely on display yet for a reason can either not be gotten as being accessible or can't be seen once perceived.

Fard, A.M et al [5]: “A New Genetic Algorithm Approach for Secure JPEG Steganography” Steganography is the demonstration of concealing a message inside an alternate message in such a path, to the point that must be caught by its planned beneficiary. Commonly, there are security operators who might want to battle these information concealing frameworks by steganalysis, i.e. finding secured messages and rendering them futile. There is presently no steganography framework which can oppose all steganalysis assaults. In this paper we propose a novel GA developmental methodology to make a safe steganography encoding on JPEG pictures. Our steganography step is in light of Outguess which is turned out to be the slightest helpless steganography framework. A mix of Out Guess steganalysis methodology and most extreme total distinction (MAD) for the picture quality are utilized as the GA wellness capacity. The model introduced here is in view of JPEG pictures; on the other hand, the thought can possibly be utilized as a part of other mixed media steganography also.

3. PROBLEM FORMULATION

Steganography is a technique for the secure transmission of data over the network. In this process, the secret information is transmitted by hiding this behind a signal or image or video. The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. In this process image is divided into different regions for the detection of least significant bits available in different images. Image pixel available in the image is a combination of three different colors red, green and blue. In the proposed work, the modified least significant bit is implemented. The main motivation behind the work which is done is to make LSB more detectable and more secure and also the data that is sent behind the audio/video is in more quantity as compared to LSB and ISB. Modifications over traditional LSB method are introduced to increase the amount of data that can be hidden in the cover image. In addition, to increase data protection our

algorithm have a built in encryption technique. As LSB the output image of algorithm will look identical to the cover image.

4. PROPOSED WORK

Image steganography is a process that has been used for hiding secret information behind any cover object. In this process information has been embedded behind least significant bits of cover object so that minimum distortion is available in the cover media during transmission. In this paper image steganography has been illustrated that contain secret image behind a cover image.

In the purposed work cover image has been selected that has been used for embedding media behind pixels of cover object. In this process image has been divided into different color space model using RGB color space. On the basis of color space regions each color band has been sub divided using discrete cosine transformation into small blocks of 8 X 8. These different blocks of the images have been used for extraction of least significant bits of the color image.

The input image that is colored is input for the system. The colored image has been decomposed into three true colors that are red green and blue.

$$A = \sum_{\substack{0 \leq i \leq m \\ 0 < j < n}} P(i, j) \quad (1)$$

This color image is combination of all the true colors that are red, green and blue. The image is decomposed into three different colors. This decomposition of the image has been done for conversion of the image into three different colors.

$$R=A (:, :, 1) \quad (2)$$

$$G=A (:, :, 2) \quad (3)$$

$$B=A (:, :, 3) \quad (4)$$

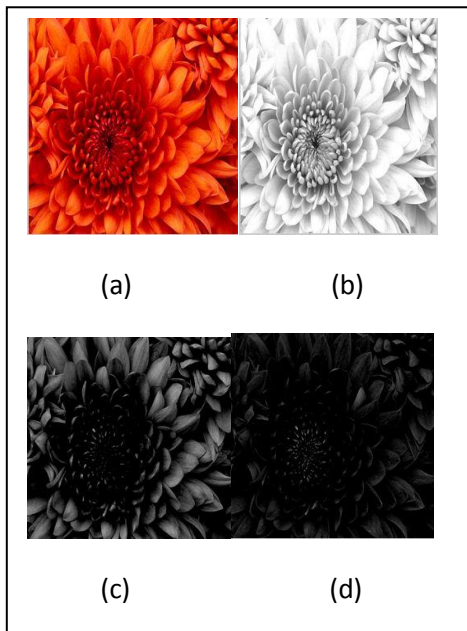


Fig 1 a) represents color image that has been taken as input, b) represents red space model, c) represents green space model and d) represents blue color space model of the image

These equations (2-4) have been used for decomposing of the colored image into three different images that contain luminance and pixel value for red, green and blue color intensities.

After decomposition the true color image into different color and image least significant bits have been computed for all the three different colors. These different color bands pixels values have been decomposed into binary format so that least significant bits from these pixels intensities can be computed.

In the purposed work multiple least significant bits have been extracted using bit streaming of the pixel value. For e.g. 158 is pixel value of a color space region then this has been divided into binary format for 8 bits. That is 10011100 in binary format. Out of this last bits from right side are least significant bits of the pixels these bits have been used for embedding secret information. These bits have been embedded using bit-XOR operation that has been used for embedding the bits of the secret data.

Secret information has been converted into binary pattern and stored in the vector format so that bits can be embedded behind these least significant bits of the cover object using XOR operation.

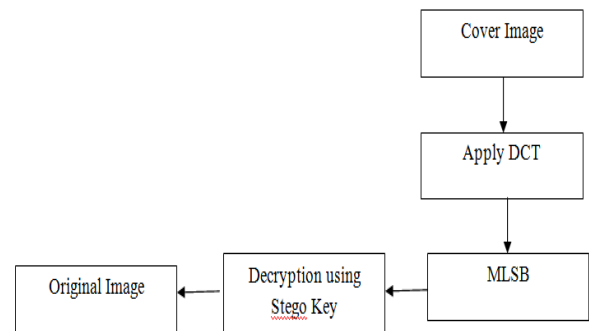


Fig 2 Flow of Work

Table 1. XOR operation

Cover Bit	Secret Bit	Result Bit
0	0	0
0	1	1
1	0	1
1	1	0

Table 1 illustrates behavior of XOR operation that has been used for embedding of secret information. In this process different image bits have been used for hiding data and create a stego image.

Algorithm steps for Purposed work

- 1) Read cover object that has been used for data hiding.
- 2) Load secret data that have to be embedding behind cover objects pixels. If the secret information is larger in size than cover object then system will represent error.
- 3) Divide cover image into different three band color subspaces using RGB splitting.
- 4) Convert secret image into vector format so that data can be embedded behind pixels of the cover image.

- 5) Input user defined key that is used as user authentication key. Embed this key behind first pixel of the red color so that on receiving end user validation can be done.
- 6) Embed secret information that is available in vector format using bit-XOR operation.

Reshape stego image pixels to form a cover image and transmit to receiver end through transmission media.

5. RESULTS

Steganography is characterized as the craft of hiding data, information or messages in a picture. Indeed the diverse record organizations can be utilized with the end goal of hiding the data like for instance the feature or sound. Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication. It is not even necessary for the two parties to agree to a specific hiding format. In the process of data hiding various approaches have been used and their performance has been evaluated on the basis of different parameters that are Peak Signal to noise ratio, MSE. On the basis of these parameter performance and real world use of an approach has been evaluated.

In the purposed work MLSB has been used with authentication key to provide secure steganography. In this process least significant bits of images have been used for data hiding. Various parameters that have evaluated for measure are described below.

5.1 PSNR

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:

$$\begin{aligned} \text{PSNR} &= 10 \cdot \log_{10} \left(\frac{\text{MAX}_1^2}{\text{MSE}} \right) \\ &= 20 \cdot \log_{10} \left(\frac{\text{MAX}_1}{\sqrt{\text{MSE}}} \right) \\ &= 20 \cdot \log_{10}(\text{MAX}_1) - 10 \cdot \log_{10}(\text{MSE}) \quad (1) \end{aligned}$$

Here, MAX_1 is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. In this expression, PSNR is inversely proportional to the MSE, if the PSNR is high then MSE is low and if the PSNR is low then MSE is high.

5.2 Mean Squared Error (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:

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

Table 2. Parameters Comparison on the basis of PSNR






Image Name	Images	Proposed Work	Previous Work
		(<i>MLSB</i>)	(<i>4LSB</i>)
Image 1		41.68	26.69
Image 2		45.69	35.40
Image 3		49.98	39.56
Image 4		53.78	48.45
Image 5		43.48	28.56

Table 2 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. PSNR represents distortion occurred in the stego object due to changes occurred in the cover image after embedding secret information. Distortion causes to noise and this can provide easily interpretation to any attacker about data hidden behind cover images pixels.

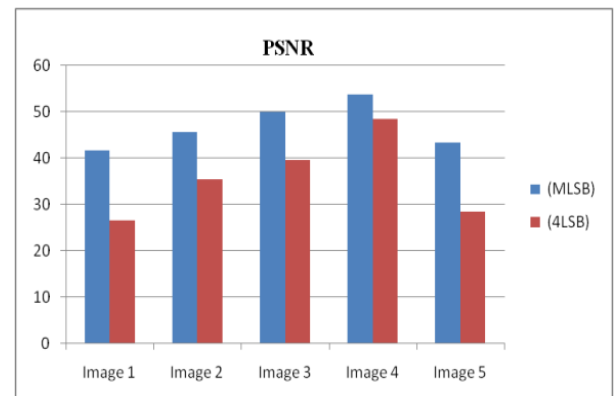


Fig.3 Comparison graph of proposed work with exiting using PSNR

Fig.3 represents graphical representation of performance evaluation parameter correlation with existing approach. Maximum value of PSNR represents minimum distortion occurred in the data after performing steganography.

Table 3 Parameters Comparison on the basis of MSE


Image Name	Images	Proposed Work	Previous Work
		(<i>MLSB</i>)	(<i>4LSB</i>)
Image 1		6.58	10.69





Image 2		2.36	9.24
Image 3		5.69	15.36
Image 4		3.59	8.69
Image 5		4.36	9.38

Table 3 represents comparison of proposed work with existing technique on the basis of performance evaluation parameters. MSE is inversely proportional to PSNR that means this compute error occurred in the image after manipulation and changes in the pixels value.

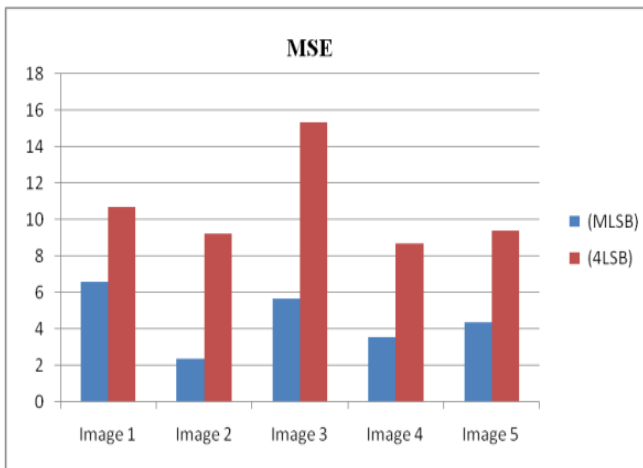


Fig. 4 Comparison graph of proposed work with exiting using MSE

Fig.4 represents graphical representation of performance evaluation parameter MSE with existing approach. MSE is minimum that means image containing maximum PSNR value. So that data those after changes contain minimum MSE and maximum PSNR provide better steganography.

Table 4 Parameters Comparison on the basis of SSIM





Image Name	Images	Proposed Work	Previous Work
		(<i>MLSB</i>)	(<i>4LSB</i>)
Image 1		0.92	0.87
Image 2		0.95	0.89
Image 3		0.98	0.93
Image 4		0.91	0.81


Image 5		0.96	0.90
---------	--	------	------

Table 4 represents comparison of proposed work with existing technique on the basis of SSIM. SSIM represents structure similarity of the stego image to the cover image after embedding secret information.

Fig.5 represents performance evaluation on the basis of SSIM with existing approach. SSIM value is lie between ranges of 0-1. That means if value of SSIM is 1 then similar image structure after embedding and if it is near to 0 then whole structure has been changed.

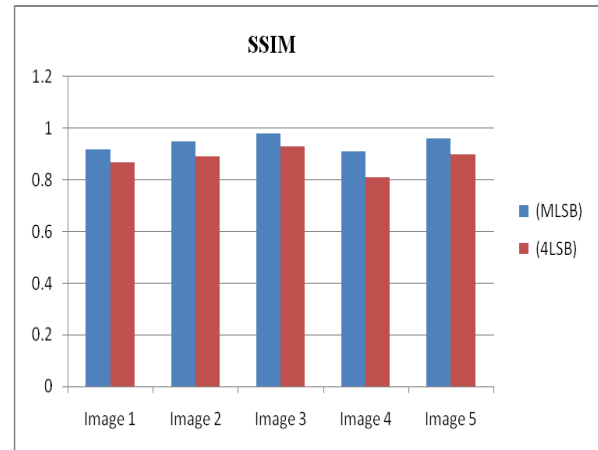


Fig 5. Comparison graph of proposed work with exiting using SSIM

Table 5 Parameters Comparison on the basis of Correlation






Image Name	Images	Proposed Work	Previous Work
		(<i>MLSB</i>)	(<i>4LSB</i>)
Image 1		0.99	0.91
Image 2		0.98	0.93
Image 3		0.99	0.92
Image 4		0.99	0.92
Image 5		0.97	0.90

Table 5 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.

Fig.6 represents graphical representation of performance evaluation parameter correlation with existing approach. As

graph represents proposed work provide better correlation than existing approach

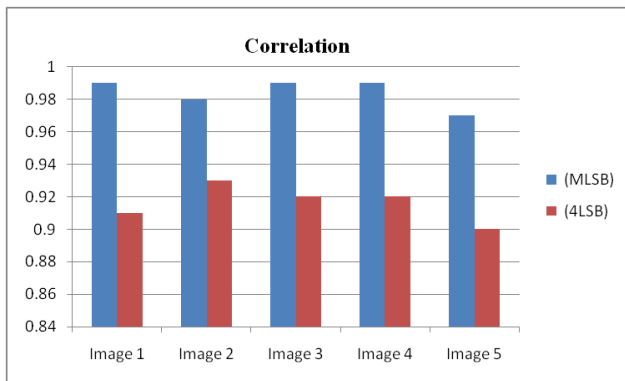


Fig. 6 Comparison graph of proposed work with exiting using Correlation

6. CONCLUSION

Steganography is the process for hiding secret information behind any cover object for secure transmission of data.

In proposed work cover object has been selected for embedding of secret information behind pixels of the object. Cover object has been divided into different color regions from a particular true color image. In the processing of division of image into separate colors red, green and blue region has been extracted from the particular image. Bit-XOR operation has been used for embedding of secret information behind the cover pixels bits. The entire color region has been used and according to intensity levels data has been embedded behind the cover pixels. To develop more secure steganography user authentication has been validated by the purposed work that embedded a onetime password during embedding process in the cover objects bits. Password has been transmitting to only authenticated user via message or mail. User authentication has been checked as the user provides the password from extraction of data. If a valid user provide correct password then he/she is able to extract data from cover object.

The purposed work has been compared with various previous approaches on the basis of performance evaluation parameters. As illustrate from results purposed work provides much secure steganography than previous LSB, 2LSB data embedding approaches. So by analyzing parameters one can conclude that purposed work provides much better results than previous approaches utilized for image steganography.

7. REFERENCES

- [1] Yang Ren-er, Tao Shun, Ding Shilei "Image Steganography Combined with DES Encryption Pre-processing" *IEEE Sixth International Conference on Measuring Technology and Mechatronics Automation*, pp. 323-326, 2014.
- [2] Guo, J.-M, Jen-Ho Chen "Quality Compressed Steganography Using Hidden Referenced Halftoning" *Ninth IEEE International Symposium on Multimedia*, pp. 273-281, 2007.
- [3] Mathkour, H, Al-Sadoon, B., Touir, A. "A New Image Steganography Technique" *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp.1-4, 2008.
- [4] Bandyopadhyay, S.K., Tai-hoonKim, Parui, S. "Network Based Public Key Method for Steganography" *IEEE International Conference on Ubiquitous Computing and Multimedia Applications*, pp. 53-56, 2011.
- [5] Fard, A.M, Akbarzadeh-T, M.-R. , Varasteh-A, F. "A New Genetic Algorithm Approach for Secure JPEG Steganography" *IEEE International Conference on Engineering of Intelligent Systems*, pp. 1-6, 2006.
- [6] Alla, K., Prasad, R. "An Evolution of Hindi Text Steganography" *Sixth International Conference on Information Technology: New Generations*, 2009, pp. 1577-1578.
- [7] Changder, S, Debnath, N.C., Ghosh, D. "A Greedy Approach to Text Steganography Using Properties of Sentences" *IEEE Eighth International Conference on Information Technology: New Generations*, pp. 30-35, 2011.
- [8] Banerjee, S, Chakraborty, M.S., Das, S. "A variable higher bit approach to audio steganography" *IEEE International Conference on Recent Trends in Information Technology*, pp. 46-49, and 2013.
- [9] Mstafa, R.J, Elleithy, K.M. "A highly secure video steganography using Hamming code (7, 4)" *IEEE Long Island Systems, Applications and Technology Conference*, pp. 1-6, 2014.
- [10] Ramaiya, M.K, Hemrajani, N., Saxena, A.K. "Security improvisation in image steganography using DES" *IEEE 3rd International Advance Computing Conference*, pp. 1094-1099, 2013.
- [11] Uddin, M.P, Ferdousi, S.J., IbnAfjal, M. "Developing an efficient solution to information hiding through text steganography along with cryptography" *IEEE 9th International Forum on Strategic Technology*, pp. 14-17, 2014.
- [12] Bugár, G., Broda, M., Levický, D. "Data hiding in still images based on blind algorithm of steganography" *IEEE 24th International Conference on Radio elektronika*, pp. 1-4, 2014.
- [13] GeHuayong, Huang Mingsheng , Wang Qian "Steganography and steganalysis based on digital image" *IEEE 4th International Congress on Image and Signal Processing*, pp. 252-255, 2011
- [14] Selvi, G.K, Mariadhasan, L. , Shunmuganathan, K.L. "Steganography using edge adaptive image" *IEEE International Conference on Computing, Electronics and Electrical Technologies*, pp. 1023-1027, 2012.
- [15] Dagar, S "Highly randomized image steganography using secret keys" *IEEE Recent Advances and Innovations in Engineering*, pp. 1-5, 2014.
- [16] Karaman, H.B,Sagiroglu, S. "An Application Based on Steganography" *IEEE International Conference on Advances in Social Networks Analysis and Mining*, pp. 839-843, 2012.