

Random Pattern based sequential bit (RaP-SeB) Steganography with Cryptography for Video Embedding

Ravpreet Kaur

CGC-COE, Landran, Department of Computer Science & Engineering, Mohali, India
Email: ravpreetkaur3@gmail.com

Manish Mahajan

CGC-COE, Landran, Department of Computer Science & Engineering, Mohali, India
Email: cgccoe.hodcse@gmail.com

Abstract—Due to an aggressive development and covert transmission of the computer users over the web, the steganography is acquiring its vogue day by day. It is the method to encode the covert data in a transmission medium in a fashion that the actuality of data must remain hidden. To protect the integrity of the data over the internet becomes necessary for the high sensitivity communications or the data transfers. The steganography carries a number of options for the embedding of the secret data into the cover data. In this manuscript, we have proposed the hybrid representation for the embedding of the data, which utilizes the random pattern embedding along with the cryptography for the higher steganography security levels. The proposed model has been designed to enhance the security level by utilizing the sequential data encoding and decoding in the video data. The video embedding creates the higher level of security for the embedded data. The experimental results have been obtained in the form of the embedding capacity, mean squared error (MSE) and Bits per Pixel (BPP). The proposed model has been found to be efficient enough for the video steganography.

Index Terms—Video embedding, sequential embedding, random pattern, secure cryptography.

I. INTRODUCTION

It is essential to use confidentiality in the transmission of the messages since the requirement of web-based applications is extremely growing. There are three methods through which the above aim can be attained; these are the cryptography, watermarking and steganography. The cryptography and steganography are completely different from each other. The prime goal of cryptography is to protect the transmissions by manipulating the encryption methods. On the other hand, the use of steganography is to conceal the messages, by which it becomes hard for the mediator to detect it [1].

The basic concern for hiding the data mainly depends on three facts: volume, secrecy, and robustness [2].

Various steganographic approaches may be used to conceal knowledge inside digital pictures with small or no visible modifications within the anticipated look of the image [1]. The benefit of using steganography is that it is mainly used for covert transmission among the two parties. The covert information can be hidden within the voice, video, text or in an image [3]. In the past, Greeks used the wax-covered tablets to conceal the information. Another technique used was that the skull of the dispatch rider was shaved and a symbol or any picture is made over there. When the hair grew back, the information would remain undiscovered as far as the head is cut down again.

Steganography defines the way in which the data is concealed that obviates the recognition of secret communication. The primary composition of steganography consists of three elements: cover image, concealed information, and the steganographic-key [16]. The cover image acts as an object where the confidential information cannot be seen.

The key is assigned to sender and receiver for encrypting and decrypting the secret information and the resultant file is the steganographic-medium file which contains the embedded information [17]. The subsequent procedure produces a very common representation of the steganographic operation:

Cover Image + Covert Data + Stego Key = Stego Object

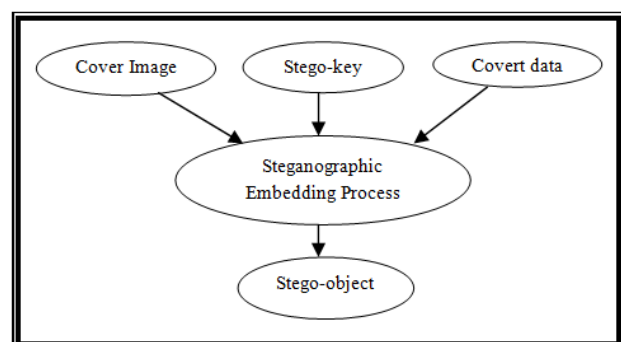


Fig.1. Process of steganography at Sender Side

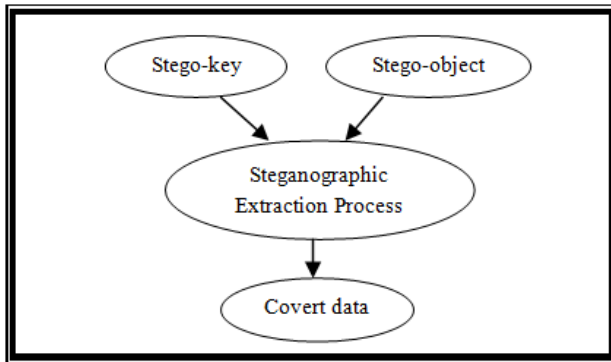


Fig.2. Process of steganography at Receiver Side

The steganographic process is divided into two parts: Sender side and Receiver side. The embedding procedure of steganography has three inputs: Covert data, Stego-key, Cover object. Once the data is embedded into the cover object, it gives the steganographic object as output. This object will be imparted to the intended receiver over the transmission medium [21]. At the receiver side, the extraction process will take place which will take the steganographic-key and steganographic-object as input. This will give the original covert (secret) data as the output.

The size of cover image must be large enough and that of the secret image should be very much smaller than it. Here the secret image can be concealed in text, audio, video or in an image. A good specimen for embedding the message is an association between recorded tracks with its lyrics. The size of the audio file in which the song is recorded is very large than its lyrics. So it's most likely to presume that compact file could be steganographically embedded into the substantial file in that manner in which that it should not influence the standard [17].

Video steganography consists of two important categories: first is to embed data in uncompressed video and the second one in the compressed video. It is well known that video consists of series of images called frames. It is the channel for transcribing, recording and relaying of active optical images. The total no. of stationary images per unit of time ranges from 6 to 8 frames per second. An executive camera has around 120 fps or even more than this. The proportion represents the size of the screen of video and its image parts.

Steganalysis is the field of discovering the existence of covert information in the cover medium. It is very exigent area since the lack of skill about certain features of the cover media can lead to the detection of the hidden messages. There are various steganographic algorithms available for the often used cover media: Audio, video, and image. Image steganalysis algorithms traverse the robust inter-pixel dependencies that are the traits of the unprocessed images [16]. Audio steganalysis algorithms are based on the trademark such as higher-order statistics etc. There are wide steganalysis methods which are used to reveal the data without following the embedding pattern and cryptographic keys [11]. Also, there are a number of available steganalysis attacks named known-cover, chosen-stego, known-stego attack, chosen-message,

stego-only and know-message, which are used to exploit the steganographic streams [14].

Attacks on the data hiding techniques have currently become an extensive hazard. For the security of the data embedded in the cover media, it can be attained to a huge level by encryption. Encryption is the method of encoding messages in such a manner that only recognized party can know about the hidden messages [7]. There are many encryption methods by which we can encrypt the secret data: Triple DES, RSA, Blowfish, Two fish, and AES. RSA is asymmetric and other four are symmetric algorithms. With the elevation in the present technology, it's currently become possible to shatter DES encrypted cipher-text. As an effect of this, Triple-DES came into existence. It encrypts the plaintext by applying DES algorithm three times. AES was instigated to substitute the 3DES because of its robust cryptographic quality. AES has three key sizes: 128,192,256 bits. This algorithm is much secured than any other algorithm [5].

There are many applications of Steganography which includes watermarking, to protect the copyright information. It is also used in security agencies, online transactions, protection of data alteration, media database system etc.

The proposed model has been designed by keeping the high-security steganography requirement on the mind. The proposed model has been designed with the highly dynamic random pattern sequential embedding for the purpose of versatile embedding, which does not incorporate the similar patterns for the embedding purposes. The random sequential pattern proposed in this paper has been designed to minimize the risk of the steganalysis attacks.

The documentation of this manuscript is as follows: Part II gives a brief intro to the techniques of steganography. Part III and Part IV gives a review concerning the Steganography Domains and Steganography Protocols. Part V discusses the literature review, Part VI describes the proposed work methodology, experimental results are provided in Part VII, and Part VIII presents the conclusion of the paper.

II. STEGANOGRAPHIC TECHNIQUES

With the emerging use of the Internet, it was important to secure the information using information technology. Various techniques have been developed to cipher and decipher the message in order to hide its meaning. The four techniques used in steganography are as follows:

Text Steganography - Text steganography [26] can be attained by changing the text format, or by changing certain features of textual elements such as alphabets. The main goal is to develop such techniques that perform changes such that that original data must be reliably decodable yet largely invisible to the reader.

Image Steganography - Images are the most accepted objects for the steganography. It overcomes the limitation of text steganography wherein it boosts the volume of the data to a large extent. It is the most widely used technique for secret communication. The size of an image varies

according to a number of pixels and the granularity of color [24]. A gray color image requires less memory space to store as compared to a color image because gray scale image is characterized by 8-bit pixel value and color image is characterized by 24-bit pixel value. To minimize the magnitude of an image to be sent, various compression techniques have been devised, such as Bitmap (BMP), Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) etc.

Audio Steganography - Information hiding in audio is based on the interpretation of sound made by Human Auditory System [26]. The steganography in audio is a challenging task because Human Auditory System (HAS) is extremely sensitive. HAS cannot interpret sound which is silent or very stressful. Some of the techniques used for audio steganography are- LSB encoding, Phase encoding, MP3 etc.

Video Steganography - A video is an association of audio and image. A continuous flow of image constitutes a video. Therefore, the techniques that can be applied to audio and image separately, they can be applied to video also. The main advantage of video is that it is comprised of a large amount of data, therefore, a small distortion in data does not put any adverse effect on video quality and it can go unobserved through human eyes [25].

III. STEGANOGRAPHIC DOMAINS

In steganography, we can work with an image in two kinds of domains:

Spatial Domain- Spatial domain approach straightly deal with the pixels of an image. To get the required augmentation, the values of the pixels are changed. The methods of the spatial domain like logarithmic transforms, power law transform depends on the manipulation of an image. The approaches of the spatial domain are especially applicable for changing the pixels values and thus the general distinction of the whole image. However, they typically magnify the entire image in a consistent way that in various instances, it gives the unpleasant results. Spatial domain techniques include Matrix embedding, LSB replacement, and pixel value differencing method [2] [1].

Transform Domain- This is the most composite method of concealing data in an image. This method is also known as the domain of embedding method. Here the procedure for embedding the information in the frequency domain is very powerful than any other domain. The advantage of frequency domain over the spatial domain is that it conceals the knowledge in that section of an image which are less revealed to image clipping, compression, and processing. The various techniques of transform domain are DFT¹, DCT² and DWT³. [1][2]

¹ Discrete Fourier Transform

² Discrete Cosine Transform

³ Discrete Wavelet Transform

IV. STEGANOGRAPHIC PROTOCOLS

Steganographic protocols [19] are divided into three classes:

- Pure Steganography
- Secret Key Steganography
- Public Key Steganography

In Pure Steganography, there is no requirement of interchanging of the steganographic key. This approach is not considerably reliable, as the sender and receiver depend barely upon the hypothesis, that another group is not aware of the concealed information.

In Secret Key Steganography, there is a swapping of the steganographic key before the transmission takes place. This system takes the cover image and embeds the covert information within it with the help of the steganographic key. On the other hand, the authorized parties who know the confidential key can converse the procedure and fetch the hidden data. As it is known that in Pure Steganography, there exists an imperceptible transmission medium; Covert Key Steganography interchanges a steganographic key that builds the system unsafe to interrupt [19]. The purpose of Secret (Covert) Key Steganography is that if the system gets interrupted then only those alliances who know about the confidential key can extricate the hidden information.

In Public Key Steganography, the system utilizes the public key cryptosystem to protect the transmission among the alliances who wants to transmit data privately. By using the public key, the sender can cipher the data, and the first entity in the key pairs called the private key which carries an association with the other entity in the key pair, called public key, can decode the hidden information. It furnishes a more powerful method of executing a steganographic system since it can use a strong technology in Public Key Cryptography. Moreover, it contains many levels of protection. The alliances must know about the utilization of Steganography and then after, they have to discover the manner to interpret the algorithm which is used by the public key system.

V. LITERATURE REVIEW

Ramalingam, Mritha et al [4], has proposed the steganographic technique for sequentially encoding and decoding the data in video images. Here most of the concealed data is transmitted by retaining the quality of video and its size as it is. So as to attain this goal, the encryption key is used data encoding and decoding sequentially. This achievement method has been calculated using the frames extracted from the video data and further extracted into the color components, which consists red, green and blue (RGB). The empirical conclusion proves that the consecutive secret writing based steganography system is easy and manufactures invisible deformation in following BMP images.

Arup Kumar Bhaumik et.al [6], the essential necessities of any knowledge concealed systems are the

security, capacity, and strength. It is extremely difficult to accomplish these all aspects simultaneously because these are reciprocally proportional to every other alternative. The authors through a spotlight on increasing the protection and capability aspects of concealed information. The concealed data technique uses immense resolution digital video as a cover medium. It furnishes the competence to cover a quite big standard of knowledge building it distinct from ordinary data hiding tools.

A.K. Jain et al. [14] has given an analysis of pattern clustering techniques from an analytical pattern identification point of view, with an objective of providing meaningful guidance and mentioning the principle ideas attainable to the wide section of clustering practitioners. It presents a classification of clustering methods and recognizes cross-cutting ideas and new improvements. The clustering problem has been addressed in numerous situations and by investigators in many disciplines; this indicates its wide appeal and adequacy as one of the steps in investigative data analysis. Clustering is a tough problem combinatorially, thereof distinction in supposition and general situations in individual groups have made the transfer of useful common conception and procedure leisurely to occur.

Saurabh Singh et al. [10] has given a brief description of a unique method of concealing image in a video. In this method, every picture elements LSB is exchanged with the one bit of the secret message. So, to seek out that if the image is hidden inside the video is a very tough job. The survey is very troublesome as the outcome of every row of image pixels is concealed inside the numerous frames of video. In this paper, LSB algorithm is described and the as a result of it, it is used in securely sending the information.

Shamim Ahmed Laskar et. al. [9] has given the technique in which the information is embedded only in the one plane of an image i.e red plane of an image and therefore the pixel is determined by employing a random number generator. It is virtually impractical to observe the alteration in an image. A steganographic key is used to seed the PRNG to determine the pixel position. Here the key importance is given to increase the security of the information and to lessen the deformation.

Gaikwad, D. P et al [3], states the evidence that steganography can be profitably enforced and can be used in the later generations of computing automation with the processing skills of image and video. It spotlights the Frame dimensions so as to create the steganographic object to create the steganographic object. The LSB methodology used here pleased the need of steganography protocols. This analysis can embody execution of steganographic formula for encrypting knowledge within video files, and also an approach to aggressively extracting that information as original.

Kumar, M. S. et al. [8] through a spotlight on concealing the covert image in a video sequence, here the hiding and extraction technique is employed. The higher order coefficients preserve the confidential information bits, the concealed information will be in the form of grayscale image pixel values. The resultant values will be

allocated to the higher order coefficient values of DCT of video frames.

Sharma, M. H. et al. [12] has worked on the two main methods of information security i.e steganography and cryptography. Both of them provide higher security to information. At first, the author encrypts the secret data by using BLOWFISH algorithm and then the encrypted data is embedded into the video using LSB approach. In this way, it becomes very hard for the unofficial human being to recognize the modifications in the steganographic-image. By using LSB, the third-party cannot retrieve the concealed information without knowing the bits of frames.

Varghese, B. B. et al. [7] has proposed the technique of embedding an encrypted data in an encrypted cover video. It certifies the security of the hidden data by encrypting it. Here the encryption is done with the XOR. Each frame of the video is also encrypted using any encryption technique. The frame key is symmetric in nature.

Savitha, N. at al. [13] has proposed a flexible steganographic system based on Fuzzy Inference system (FIS) and Human Visual System (HVS). The Mamdani and Sugeno techniques of the fuzzy inference system emerges and negotiate that although they both performs alike functions but the execution time of the Sugeno is very less as compared to Mamdani. As a result, there is an increase in Peak signal to noise ratio.

Pujari, S. et al. [18] has worked with the LSB approach which is used to embed the alphabets of the confidential text information in the image file however before embedding, the whole text is split. All the parts of the text are put into distinct areas of the cover object in a random fashion. A pseudo-random sequential pattern generator task is performed to embed every part of covert information into the blocks of the cover object in a random manner.

Seth, S. M. et al. [21] has done the relative investigation of the three algorithms; RSA, DES, and AES by acknowledging specific variables like computing time, memory management, and output byte. These variables are an important crucial matter of concern in any Encryption Algorithm. The exploratory outcome shows that DES method utilizes minimum reaction time for encryption and the AES method has minimum utilization of memory. The time distinction in the case of AES and DES algorithm is extremely small. RSA algorithm utilizes extended runtime memory and the time taken for encryption management is also immensely high for the overall output byte size is minor in this algorithm.

Kumar, P.M. et al. [22], has proposed the image steganographic method which includes edge-based detection approach. The authors consider some smooth areas, which affects the LSB of cover objects not to be in random fashion. If the information is embedded in these areas, the LSB of the steganographic object becomes random and easy to identify. They produce a new technique which conceals the files in an image.

VI. PROPOSED WORK

The proposed work for the security of image has been formulated into 3 stages as shown in the fig. below. These are image compression, image encryption, and steganography.

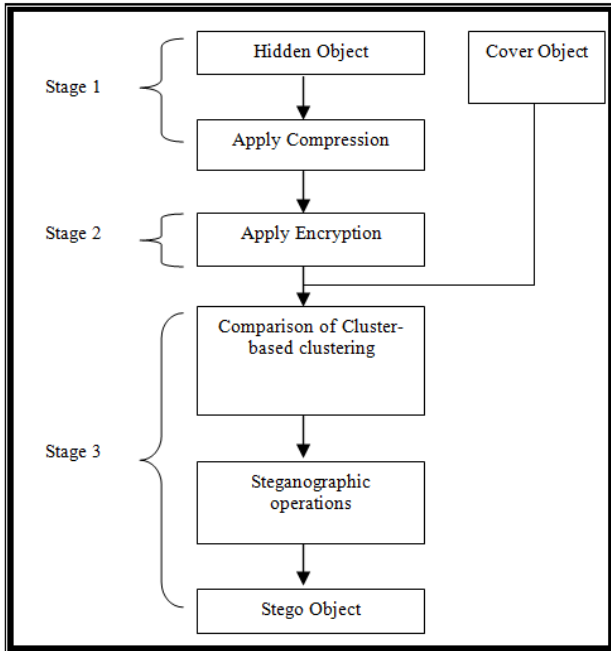


Fig.3. Workflow for the proposed model

In the first stage, the hidden object is reduced to its size. The reason behind reducing the size of an image is that it accelerates to less increase in the memory during embedding. The second stage is the encryption of an image. Now the compressed image is encrypted to provide another layer of security, which makes the security stronger. Here in this stage, color clustering is used, on the basis of which the concealed data is embedded into the cover image.

1. **Image Compression** - There are various compression techniques available which include DCT, DFT, and DWT. For jpeg images, DWT is preferred over DCT and DFT. Although it is complex, it has higher compression ratio. By using DWT, the overall count of the transform coefficients gives the same as the count of the input samples extracted from the original image. To reduce no. of bits, all subbands are quantized. The signal or image quantization can be achieved by utilizing the uniform scalar quantization along with its origin from the dead zone. The formula for the uniform scalar quantization in the dead-zone can be given by the following equation:

$$q_k(a, b) = \text{sign}(y_k(a, b)) \left\lfloor \frac{|W_k(a, b)|}{\Delta_k} \right\rfloor \quad (1)$$

where $W_j(m, n)$ depicts the DWT coefficients in the frequency sub-band j and ∇_j gives the step size for quantization for the dedicated subband j .

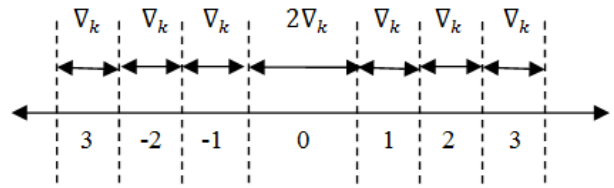


Fig.4. Dead-zone quantization about the origin.

2. **Encryption of an Image using Blowfish** - To encrypt the secret image, blowfish algorithm is used to conceal the details of the image of hidden object. Blowfish algorithm is considered as the fastest one among all other algorithms.

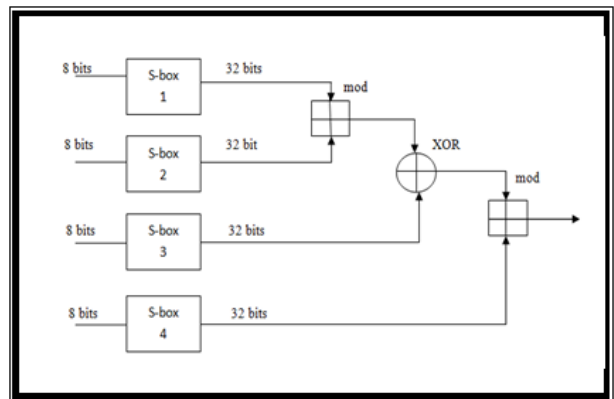


Fig.5. Blowfish encryption for image processing

3. **Steganography**- Steganography is a security technique which is used to conceal the data into another object which can be a text, image, audio, video etc.

3.1. Working of Color Clustering Based steganography:

A. Clustering:

The groups of similar objects are called a cluster. Here objects have a similarity with each other object in the cluster itself but dissimilar with the objects of other clusters. Clusters always contain useful information.

B. Pattern Matching using Color:

Clusters are created with the help of pattern matching using color. Here a color palette is used for comparing the color with the color of the pixel. When clustering is applied to the image, after that the selection of the cluster takes place in which the concealed message has to be embedded. After embedding, clusters are placed at a proper position to form an image. Now, this image is sent to the receiver and reverse process is applied. Here steganographic-image will be the input, pattern matching will be applied to it and clusters will be identified in which the message is embedded. After that message bits

will be extracted and are combined to get readable and meaningful information.

VII. EXPERIMENTAL RESULTS

Tentative outcome evaluates the performance by concealing the information in a cover image using MATLAB. To assess the execution of the proposed model, different performance parameters are used. These are:

- Embedding capacity – It's the payload capacity of the steganography strategies that characterizes the capability of the steganographic representation for embedding the precise quantity of data.
- Flexibility: The steganographic capability of the steganography algorithm to manage different groups of the information beside the varied operations such as cropping, filtering, rotations, and compression
- Imperceptibility: The quality of the steganography is measured by the variables to outline the quality of the embedding in the terms for recognizing and discovering the information embedding through the steganalysis methods
- Bits per pixel- The quantity of bits of data stored per pixel of an image or exhibit by a graphics adapter. The more bits there are, the more colors can be portrayed, and however, a lot of memory is needed to store or to show the image. A color is delineated by the intensities of red, green and blue (RGB) elements.
- Peak signal to Noise Ratio- It is defined as the proportion between the extreme possible power of a signal and the power of distorting noise that influences the quality of its representation.






$$PSNR = 10 \log\left(\frac{C_{max}^2}{MSE}\right) \quad (2)$$

- Mean Square Error - The mean squared error (MSE) is the overall error based upon the difference of the matrix pixel count between the ground truth image (cover image) and steganographic image created after the embedding process.

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \quad (3)$$

The various classifications of the images have been tested beneath the experiments in the following Table 1. In-depth verification of the proposed model has been assessed over the image data contained from the 10,000 images in the Prof. Wang's dataset.

Table 1. The performance evaluation of proposed model

| Image Dataset | PSNR (Hidden Image) | MSE (Hidden Image) |
|------------------------------------------------------------------------------------|---------------------|--------------------|
|  | 45.14 | .00975 |
|  | 48.74 | 0.0089 |
|  | 46.55 | .0021 |
|  | 43.10 | .0015 |
|  | 47.24 | 0.0056 |

The above reading has been obtained from the experiments conducted on the proposed steganographic model. The image dataset has been randomly chosen from the 10,000 images in the five major categories from the various environments. The images are obtained in the testing selection with the random means and include the images of good resolution from urban scenes, people, nature and digital categories. The images based upon the various color illumination effects, different lighting, grayscale, one color distribution, etc has been tested under the proposed model. The following graph has been plotted on the basis of the reading obtained from the table 1.

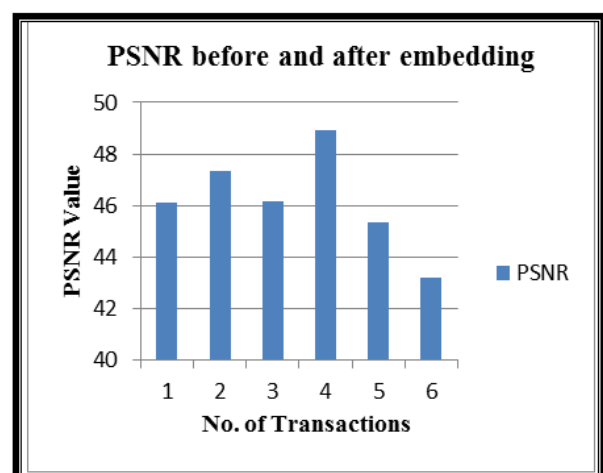


Fig.6. Evaluation of the proposed model based upon PSNR

PSNR depicts the standard of the image by doing image comparing, before and once processed on the chosen image information. The graph shown above has evidently shown that the value of PSNR is higher for all the image groups in the dataset, that shows proposed algorithm generates a coherent image at the end of the processing.

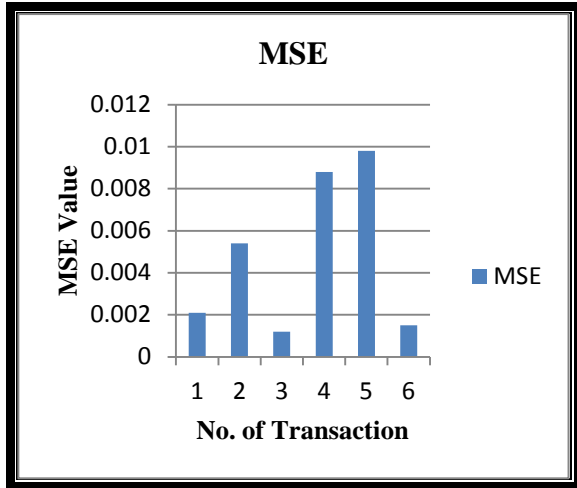


Fig.7. Comparative analysis of proposed model based upon MSE

Mean squared error depicts the overall error in the received information when it is compared to the data before it is processed and once it is processed. MSE value should be less to delineate the bare damage to the quality of an image. In the graph shown above, the value of the MSE value is lower for various image categories in the image dataset.

The experiment has also been taken out in figures 6(a) and 6(b) by embedding a message which includes ASCII characters.

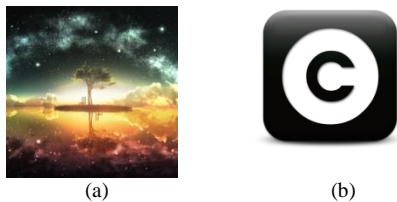


Fig.8. (a) Cover Image and (b) Secret Image



Fig.9. Stego Image

• **Embedding capacity**

The embedding capacity of the cover image is calculated by measuring the pixel density of the cover image and the bit value measured according to the count of the embedding values. The embedding capacity reveals the actual capacity of the image to embed the given data size.

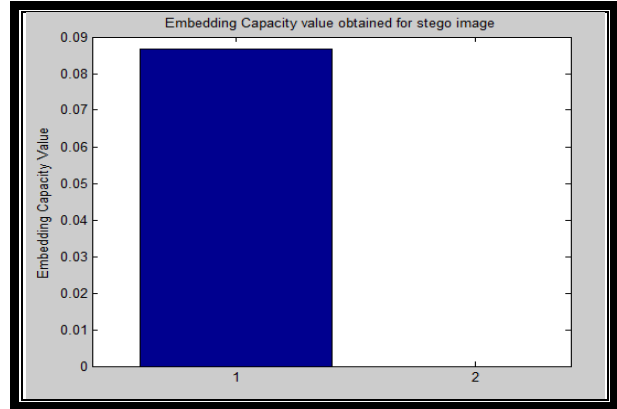


Fig.10. Embedding capacity index obtained for the steganographic image to embed the cover image

The embedding capacity of the input image has been measured between 0.08 and 0.09 ratio of the original image, which reveals the robustness of the embedding algorithm to embed the given data. The given embedding capacity has shown the least probability of detection of the embedding signature of the input data in the steganographic image created after the whole steganography process.

• **Bits per Pixel**

Bits per pixel shows the bits used in the cover image to embed one pixel of the input covert image. The bits per pixel (bpp) evaluate the capacity of the cover image to embed the secret image. The higher bits per pixel value increases the level of the security against the detection attacks and steganalysis attacks over the steganographic image. The bpp values have been obtained between 45 and 50 bits, which way higher to embed the smaller secret image in the cover image in order to return the steganographic image with the embedded data

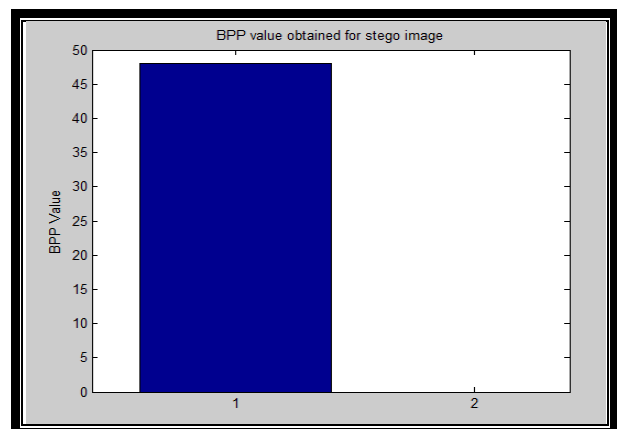


Fig.11. Bits per pixel obtained according to the embedding capacity

• **Mean Squared Error**

The mean squared error (MSE) is the overall error based upon the difference of the matrix pixel count between the ground truth image (cover image) and steganographic image created after the embedding process. The mean squared error reveals the difference

between the cover image and steganographic image, which shows the effect of embedding over the image matrix. The difference is measured in the ratio of change in the image matrix due to the embedding factor.

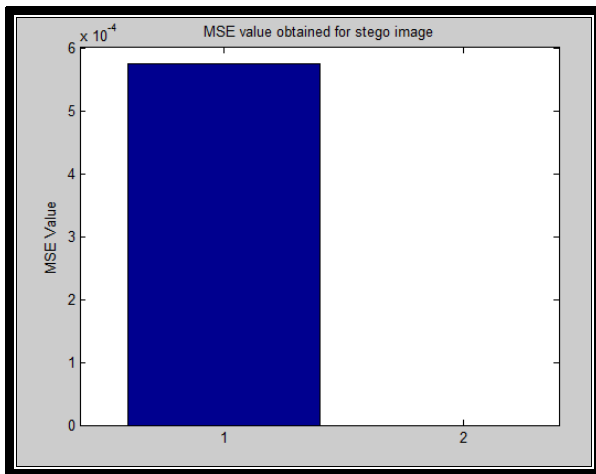


Fig.12. Overall mean squared error

The mean squared error value has been obtained nearly at 6×10^{-4} , which is computed the cover image before and after embedding process. The value of 0.0006 or 6×10^{-4} reveals the minimum change occurred in the matrix due to the embedding effect. The 1080p based cover image has been utilized for the embedding of the secret image, which is considered best for embedding of the secret data with the minimum probability of detection through steganalysis attacks.

VIII. CONCLUSION

The proposed model is based upon the multiple rule-based embedding in the cover data for the higher embedding security against the steganalysis attacks. This model focuses upon the compatibility verification between the cover image and the secret image in order to find the adaptable match for embedding. The proposed model has been guided to defer the embedding process if the compatibility is not certainly matched and does not satisfy the given set of thresholds. This procedure is responsible for the robust evaluation of the overall security embedding by accepting the adaptable cover image match only. This model increases the level of security which is clearly indicated by the mean squared error and bits per pixel based parameters under the result analysis sections. Several experimental results have been conducted in order to evaluate the overall system performance, which can be clearly aforesaid as the robust embedding option as it clearly decreases the risk of the data divulgence attacks over the steganographic objects.

ACKNOWLEDGMENT

The authors wish to acknowledge the Management of CGC-COE, Landran, Mohali, India. This research paper is made possible through the help and support from everyone including teachers, parents, family, and

friends. We would like to convey our sincere thanks to our HOD Sir (Mr. Manish Mahajan) for motivation and guidance. The organization has provided research environment, and their faculties and scholars from the department of CSE, CGC-COE, Landran provided precious suggestions during the investigation and research work.

REFERENCES

- [1] Thakara, S. S., Bhale, N.L. (2014), "A Review of Digital Image Steganography Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(6), pp. 465-471
- [2] Sharma, S., & Kumar, U. (2015), "Review of Transform Domain Techniques for Image Steganography," *International Journal of Science and Research*, 2(2), 1, pp. 194-197
- [3] Gaikwad, D. P., et al. "Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithms in Video Steganography," *International Journal of Engineering Research and Applications (IJERA)*, 1(2), pp. 102-108
- [4] Ramalingam, M., and Isa, N. A. M. (2014, October), "A steganography approach for sequential data encoding and decoding in video images," *Proc. IEEE International Conference on Computer, Control, Informatics, and Its Applications, 2014*, pp. 120-125.
- [5] Penchalaiah, N., & Seshadri, R. (2010), "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES).," *International Journal of Computer Science and Engineering*, 2(05), pp. 1641-1645.
- [6] Bhaumik, Arup Kumar, et al. (2009), "Data hiding in a video." *International Journal of Database Theory and Application* 2.2, pp. 9-16.
- [7] Varghese, B. B., & Haroon, R. P. (2014), "Reversible Encrypted Data Hiding In Encrypted Video", *IOSR Journal of Computer Engineering (IOSR-JCE)*, 16(1), pp. 71-82.
- [8] Kumar, M. S., & Latha, G. M. (2014), "DCT Based Secret Image Hiding In Video Sequence," *International Journal of Engineering Research and Applications ISSN, 2248-9622*, 4(8), pp. 05-09
- [9] Laskar, S. A., & Hemachandran, K. (2013), "Steganography based on Random Pixel Selection for Efficient Data Hiding.," *International Journal of Computer Engineering and Technology*, 4(2), 31-44
- [10] Singh, Saurabh, and Gaurav Agarwal, (2010), "Hiding an image to a video: A new approach to LSB replacement." *International Journal of Engineering Science and Technology* 2.12, pp. 6999-7003
- [11] Meghanathan, N., & Nayak, L. (2010), "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media," *International journal of Network Security & Its application (IJNSA)*, 2(1), pp 43-55.
- [12] Sharma, M. H., Mithlesh Arya, M., & Goyal, M. D. (2013), "Secure Image Hiding Algorithm using Cryptography and Steganography," *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN, 2278-0661*.
- [13] Savitha, N., Srinath N. K., Usha B. A., (2015), "Fuzzy Logic Based Parallel Data Embedding Technique for Image Steganography," *International Journal Of Current Engineering And Scientific Research (IJCESR)*, 2(9), pp.109-113
- [14] Richer, P. (2003), "Steganalysis: Detecting hidden information with computer forensic analysis," *SANS/GIAC*

Practical Assignment for GSEC Certification, SANS Institute, 6.

- [15] Jain, Anil K., M. Narasimha Murty, and Patrick J. Flynn, (2006), "Data clustering: a review." *ACM computing surveys (CSUR)* 31.3: 264-323
- [16] Vyas, K., Pal, B. L. (2014), "A Proposed Method in Image Steganography to improve Image Quality with LSB technique," *International Journal of Advanced Research in Computer and Communication Engineering* 3(2),5246-5251
- [17] Khosla, S., & Kaur, P. (2014), "Secure Data Hiding Technique using Video Steganography and Watermarking," *International Journal of Computer Applications*, 95(20), pp. 7-12.
- [18] Pujari, S., & Mukhopadhyay, S. (2012), "An Image based Steganography Scheme Implying Pseudo-Random Mapping of Text Segments to Logical Region of Cover Image using a New Block Mapping Function and Randomization Technique," *International Journal of Computer Applications*, 50(2).
- [19] Sheelu, & Ahuja, B. (2013), "An overview of Steganography IOSR Journal of Computer Engineering," 11(1), pp.15-19.
- [20] Seth, S. M., & Mishra, R. (2011), "Comparative Analysis Of Encryption Algorithms For Data Communication 1, 4(2)
- [21] Panjabi, P. K., & Singh, P. (2013), "An Enhanced Data Hiding Approach using Pixel Mapping Method with Optimal Substitution Approach," *International Journal of Computer Applications*, 74(10), pp. 36-43
- [22] Kumar, P. M., & Shunmuganathan, K. L. (2012). Developing a secure image steganographic system using TPVD adaptive LSB matching revisited algorithm for maximizing the embedding rate. *Information Security Journal: A Global Perspective*, 21(2), 65-70.
- [23] Jain, A., & Gupta, I. S. (2007, October), "A JPEG compression resistant steganography scheme for raster graphics images," *IEEE Region 10 Conference* (pp. 1-4). IEEE.
- [24] Hamid, N., Yahya, A., Ahmad, R. B., and Al-Qershi, O. M. (2012), "Image steganography techniques: an overview", *International Journal of Computer Science and Security (IJCSS)*, 6(3), pp.168-187.
- [25] Por, L. Y., and Delina, B. (2008, April), "Information hiding: A new approach in text steganography," *Proc. International Conference on Mathematics and Computers in Science and Engineering*, vol. 7, World Scientific and Engineering Academy and Society.
- [26] Jayaram, P., Ranganatha, H. R., and Anupama, H. S. (2011) "Information hiding using audio steganography—a survey," *International Journal of Multimedia & Its Applications (IJMA)*, vol. 3, 86-96.
- [27] Dickman, S. D. (2007), "An Overview of Steganography," *Department of Computer Science, James Madison University Infosec Techreport*, vol. 2, pp. 305-315.

Authors' Profiles



Ravpreet Kaur, she is pursuing M.Tech in CSE from CGC-College of Engineering, Landran, Mohali. She received her degree of Bachelor of Technology in CSE from CGC Gharuan(Chandigarh University) , Mohali in 2014. Her area of interest is Digital Image Processing.



Manish Mahajan, he is pursuing P.hd from PTU. He received his degree of M.Tech in CSE in 2006 from PTU and B.Tech (IT) in 2004 from Kurukshetra University in 2004.

Currently, he is an associate professor and HOD of CSE in CGC-COE, Landran. He is having more than 11 years of teaching experience and more than 5 years of research experience.