I.J. Education and Management Engineering, **2017, 1, 54-64**
Published Online January 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2017.01.06

Available online at http://www.mecs-press.net/ijeme

Random Pattern Standard Bit Embedding for Minimized Histogram Difference

Ravpreet Kaur[a], Manish Mahajan[b]

[a] *Research Scholar,CGC-COE, Landran, Mohali,India*
[b] *Head of Department, CGC-COE, Landran,Mohali, India*

Abstract

The rapid development of the transfer of data via internet made it easier to send the correct information and quicker to the destination. Today's massive demand of web applications needs the information to be communicated in a secure manner. The transmission of information in a public communication system isn't secure because of interception and improper manipulation by an eavesdropper. So for this problem, the solution is Steganography, which means the art of hiding information in ways that avert the revealing of hiding messages. Secure video steganography is a difficult task of sending the embedded data to the receiver without being detected. This paper presents a steganographic model which is based on random pattern based sequential bit encoding. The proposed model has been designed to enhance the security level. The video embedding creates the higher level of security for the embedded data. Here the encrypted secret image is embedded into the blocks of a cover video file which is selected using autocorrelation function which measures the similarity between the two images. The embedding is done on the basis of random selection of the pixels in the blocks of cover video. The performance parameters that are used to obtain results are taken in the form of chi-square histogram difference measurements. The proposed model increases the security by using random pattern embedding.

Index Terms: Video steganography, cover video, random pattern, autocorrelation, chi square.

1. Introduction

Due to the detonation of the web programs, it leads mankind into the digital world and the transmission which is done through digital information gets repeated. Although some difficulties emerge and have been traversed such as security of the information in digital transmission, hidden transmission by means of a digital channel.

Steganography is the robust information hiding approach for concealing confidential data within another file. Steganography term is usually obtained from the Greek language – which means secret writing. It is the science

of unrevealed transmission which is used to hide confidential data within any cover medium like text, audio, video or image files in the way that only authorized users can have access to identifying the concealed information [3].

Steganography and cryptography are extensively used methods to conceal information so that the existence of message is not known to anyone. Steganography has become the most prominent means for transmitting data secretly in contrast to the cryptography. In both approaches, the hidden information is communicated between the sender and the recipient. In cryptography, the information is made obscure so that third party cannot judge the data. On the other hand, steganography points to conceal information and covert transmission. Steganography conceals the secret data in video, text, image or in audio file [22].

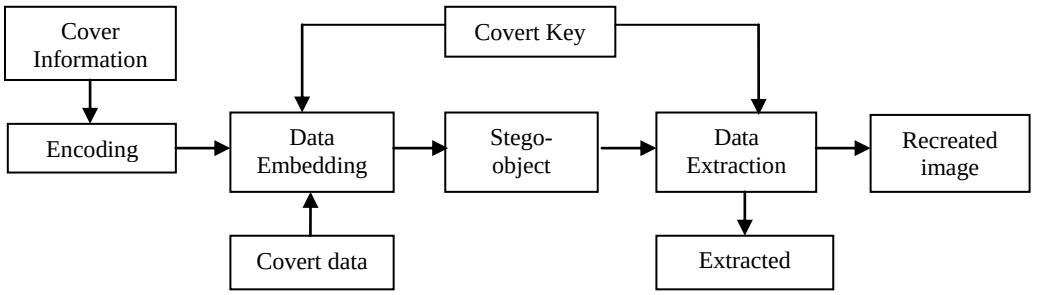

Fig.1. Fundamental View of Steganography System

In Fig. 1, the fundamental view for the steganography system is shown. Here the original image is encoded with the covert data and the covert key is embedded into the secret data. On obtaining the stego-image, the hidden data is extracted using the same key [23]. The size of the cover image must be large so that it can hide sufficient amount of data and that of the secret object must be small enough.

The file formats used in steganography are image, audio, video and text. Images are the most used file format, but its restricted size limits the volume of embedding. In case if large no. of unrevealed data has to be transmitted, then image steganography will not fit for that purpose. Therefore the technique that has higher embedding size will be taken into account. Digital video is made up of frames and also has greater signal space, so video steganography will have higher volume [4].

Data embedding can be used to keep the data within any cover-medium. Reversible data hiding certifies that the cover image should not be changed after the decryption and extraction of the data [6]. For the secure distribution of information, encryption is used. By using this, exclusively the intended sender and receiver would be allowed to retrieve the encrypted information. Encryption can be categorized into symmetric or asymmetric according to the keys being used. If the two schemes i.e. data hiding and encryption are combined, it will result in providing more security and secure communication [6].

There are many methods of steganography for embedding the data in images. Various methods of embedding the data are based on the process of exchanging the least-significant bits of the pixels of the cover image and the procedure of randomly generating a number are generally used to attain security [17].

Steganographic techniques based on image and video are often categorized into following domains:

- **Spatial Domain Method**: In this approach, the unrevealed data is straightly embedded into the pixel's intensity i.e. some of the values of the pixel of the image are modified at the time of concealing data. This approach has been categorized into Least Significant Bit, Pixel Value Differencing, Random Pixel embedding method etc. [14][8]
- **Transform Domain Method**: Here the concealed information is embedded into the frequency domain of the cover medium. It is the complicated manner of concealing knowledge in an image. Several designs and modifications are used for obscuring the information in an image. The categories of this technique are

Discrete Cosine transform (DCT), Discrete Wavelet transform (DWT), Discrete Fourier transform (DFT) etc. [14]. This approach is more advantageous than spatial domain because they obstruct the message in that region which is less revealed to compression, and processing of an image [10].

- **Distortion Method**: Here in this approach the information of the cover image is required in the process of decoding where the decoder inspect the distinction among the initial cover object and the distorted cover object to recover the concealed data [11]. A series of adaptation is applied to the cover object in order to obtain the steganographic image. This series is used to match the concealed data which is to be transmitted.
- **Masking and Filtering**: This method works in the same way as the paper watermark does. In this, the data is obstructed by marking an image by using the sound levels of the cover object. The methods of watermarking are more integrated into an image; therefore they can pertain without having the fright of demolition of an image. [11].

There are various attacks on steganography. Some of them are listed below [5][12]:

- **File Only**: The assailant has access to the file and he ascertains that the information is hidden within the message.
- **Multiple Encoded File**: The assailant has m distinct copies of the files with m distinct information. For eg. If the company has to insert different data into all files; the assailant may try to exchange the data with their own data.
- **Random Tweaking Attacks**: An assailant can add arbitrary modifications to all the files in the expectation of demolishing the information.
- **Destroy Everything Attack**: The assailant could solely demolish the message.
- **Visual Attack**: This attack is known as the steganographic-only attack that removes the chunk of the information in such a way that it permits the person to look for visual inconsistency.

Video Steganography can be categorized into two principal categories. The first one is to embed data in the uncompressed video and the second one is to embed the information straightly into the compressed video [2]. Generally, a video consists of a set of frames which are played at bounded frame rate based on the standards of the video. There are various parameters by which the quality of video can be measured like no. of pixels in an image, the size of the frame and frames per second (fps) [7].

Steganalysis is the procedure of determining steganography by investigating different parameters of the steganographic object. The first step for this procedure is to recognize the suspected steganography media. By following this, it will discover whether the concealed information is contained within the steganographic object or not; after that, it will try to retrieve the information from it [9].

The techniques of steganography are classified into two categories: active and the passive techniques. In the former one, the type of the information inserted is extracted, and in the later one, the existence or non-appearance of the concealed information is examined [22].

The proposed algorithm has been designed by taking into account the need for security. It has been made using random pattern based sequential bit encoding where the image is concealed anywhere in the video. The embedding in a video creates a high level of security.

The paper is organized as follows. Part 2 discusses the literature review. Part 3 formulates the problem of the system. Part 4 describes the proposed algorithm. Experimental results are provided in Part 5 and Part 6 presents the conclusion of the paper.

2. Related Work

Shakir, Ahmed C. [19], the inadequate communication over the ubiquitous network is generally approved using digital file formats such as audio, text, video and images on the web. Straightly masking the contents of the

information by applying cryptography was not fair. It gives another sheet of security by covering the data. To give more security, there are various procedures which are used in steganography for concealing the secret knowledge inside the digital color electronic image. The quadratic approach is used in cryptography and the integration between cryptography the area accomplished by the binary image, adjacent to the public key and steganography producing unaffected data.

Ramalingam, M. et al [15], has proposed the steganographic method for encoding and decoding the data sequentially in video images. By maintaining video standards and its size, the secret information can be transferred. To achieve this target, the use of encryption key is required for data encoding and decoding sequentially. This procurement has been deliberated by manipulating video images in bit mapped (BMP) format in Red, Green, and Blue (RGB) peripherals. The actual conclusion demonstrates that the successive secret writing based steganography system is straightforward and creates indiscernible distortion in the BMP images.

Sherly, A. P. et al. [2], has proposed a compact video Steganographic strategy. Here the information is concealed in the compressed domain. The information is embedded into large blocks of I, P and B-frames with an extreme size of motion vectors. To amplify the volume of the concealed knowledge and to give an invisible steganographic image for individual's sight, a novel embedding process called Triway pixel-value differencing (TPVD) is devised. This algorithm can be implemented on compressed videos without any breakdown in the standard of the video.

Laskar, S. A. et al. [10] method, information is embedded into the red plane of the image and by using a random number generator, a pixel is selected. It is virtually impracticable to observe the alterations in the image. A stego key uses PRNG (pseudo-Random Number Generator) to choose the location of the pixel. This paper gives emphasis on raising the security of the information and to diminish the deformation rate.

Sharma, M. H. et al. [18] has worked on the two fundamental techniques of data security i.e steganography and cryptography. Both of them furnishes higher security to the information. Firstly, the author encrypts the confidential data by using BLOWFISH algorithm and then the encrypted data using LSB method, is embedded into the video. In this way, it becomes very tough for the unauthenticated person to identify the refinement in the stego-image. By using LSB, the third-party will be unable to recover the hidden data without knowing the bits of frames.

Kumar, M. S. et al. [16], concentrated on concealing the hidden image in a video sequence. He used hiding and extraction approach. The higher order coefficients preserve the bits of hidden information, the secret message will be in the form of grayscale image pixel values. The outcome will be the binary values which will be allocated to the high ranking coefficient values of discrete cosine transform of video frames.

Divya, K. P. et al. [20] has given a new approach to conceal the image in the video frames. The frames are selected in a random manner to embed the image. Thus, when the invader tries to extract the frames from video, he will not be able to spot the occurrence of the image which was put within the frames. Further, the video is taken as one of the best provision to embed the image because the size of an image is large. It furnishes high-level security to the transferred image. The use of LSB algorithm is made to embed the image into the frames of video.

Kumar, P.M. et al. [13] has worked upon an image steganographic approach which incorporates an edge based strategy. There is an occurrence of few smooth areas in unprocessed images, which in results prompt the LSB of original images not either to be random or to comprise knowledge as in the prominent bit planes. The LSB of the steganographic images gets random in nature if the information is embedded in those smooth areas, and it would be much easier to recognize it. The authors present a new technique which obscures the file in images.

Juneja, M. et al. [24] presents a secured sturdy technique of security of information. It provides two sections based LSB approaches for embedding the secret information in the LSB's of the blue part and some of the green part of the random pixel position on the edge of images. A new method for information embedding based on the information accessible in MSB's of the RGB section of the pixels selected randomly beyond smooth regions. On integrating it with an AES encryption, it becomes more powerful. The capacity and the value of the

PSNR also raises high.

Pujari, S. et al. [21] uses the LSB method for embedding the letters of the concealed text information into an image. But before the embedding is done, the whole text is divided into chunks and each one of it is randomized at the bit level. All the chunks of the text are put into distinct areas of the original or cover image in a random way. A pseudo random pattern is generated to embed the each component of the concealed message into the blocks of the original image randomly, using the random sequence generator function.

Gaikwad, D. P et al [3], says that the steganography can be applied productively and can be used in the subsequent types of computing automation with the processing expertise of an image and video. It emphasizes the Frame dimensions in order to generate the steganographic object. The procedure of LSB used here requires steganography protocols. This research can manifest the accomplishment of steganographic solution for ciphered information within video data, and also a procedure to aggressively extracting that data as initial.

Singh, S. et al. [10] has given a distinctive approach of hiding an image in a video. In this approach, each LSB pixel is changed with one bit of the covert information. To find whether the image is hidden inside video is a very hard task. The investigation is extremely inconvenient by virtue of which each row of image pixels is invisible inside the several frames of video. Here in this paper, LSB algorithm is represented and it is being used in sending the data secretly.

Jain, Y. K. [26], has proposed an adaptive least significant bit spatial domain embedding technique. This technique divides the image pixels ranges (0-255) and produces a steganographic key. This private stego-key has five distinct gray level ranges of an image and each range indicates to substitute fixed number of bits to embed in the least significant bits of an image. The capability of proposed approach is its integrity of concealed hidden data in a stego-image and high hidden capacity. The limitation is that for the purpose of integrity, the extra bits of signature have to be concealed within the hidden message. A technique for the color image is also proposed only to change the blue channel with this idea for information hiding. This technique is directed to attain high hidden capacity and the security of the secret message.

3. Problem Formulation

The main problem with the existing model exists in the Steganography application and the data encryption process. The existing model has been analyzed thoroughly for its core problems. The main problem with conventional key cryptography is that it is a very hard job to keep symmetric key safe from people other than sender and receiver. If sender and receiver are far away from each other and they have not shared the secret key, then third party or courier must be trustworthy to transfer the key to the intended receiver only. Also, the existing model is based upon the sequential bit encoding with the fixed pattern which always makes it vulnerable to steganalysis attacks. In the case of encryption, this model is not secure as it uses the XOR operations for the encryption process. The XOR operation based encryption model is considered very weak against several cryptanalysis attacks to decode the encrypted data without using the encryption key [12].

4. Algorithm Design

The frequency embedding method has implemented using Progressive Exponential Clustering algorithm. In this algorithm:

- First, the clusters are created based on color pattern matching. An exhaustive search is conducted to pair up the same color pixels within a cluster. Each pixel which is similar in color within threshold value is included in a cluster.
- After the clusters are created, their color table is created based on color clusters.
- As it is very rare that two or more clusters can be of the same size, therefore, the cluster which contains the largest number of pixels is chosen so that embedding space should be as large as possible.
- After the message is embedded, the steganographic image is generated. Here AES- based cryptographic

algorithm would be implemented to create the more secure hidden object.

The general principle of this algorithm is shown in figure 2.

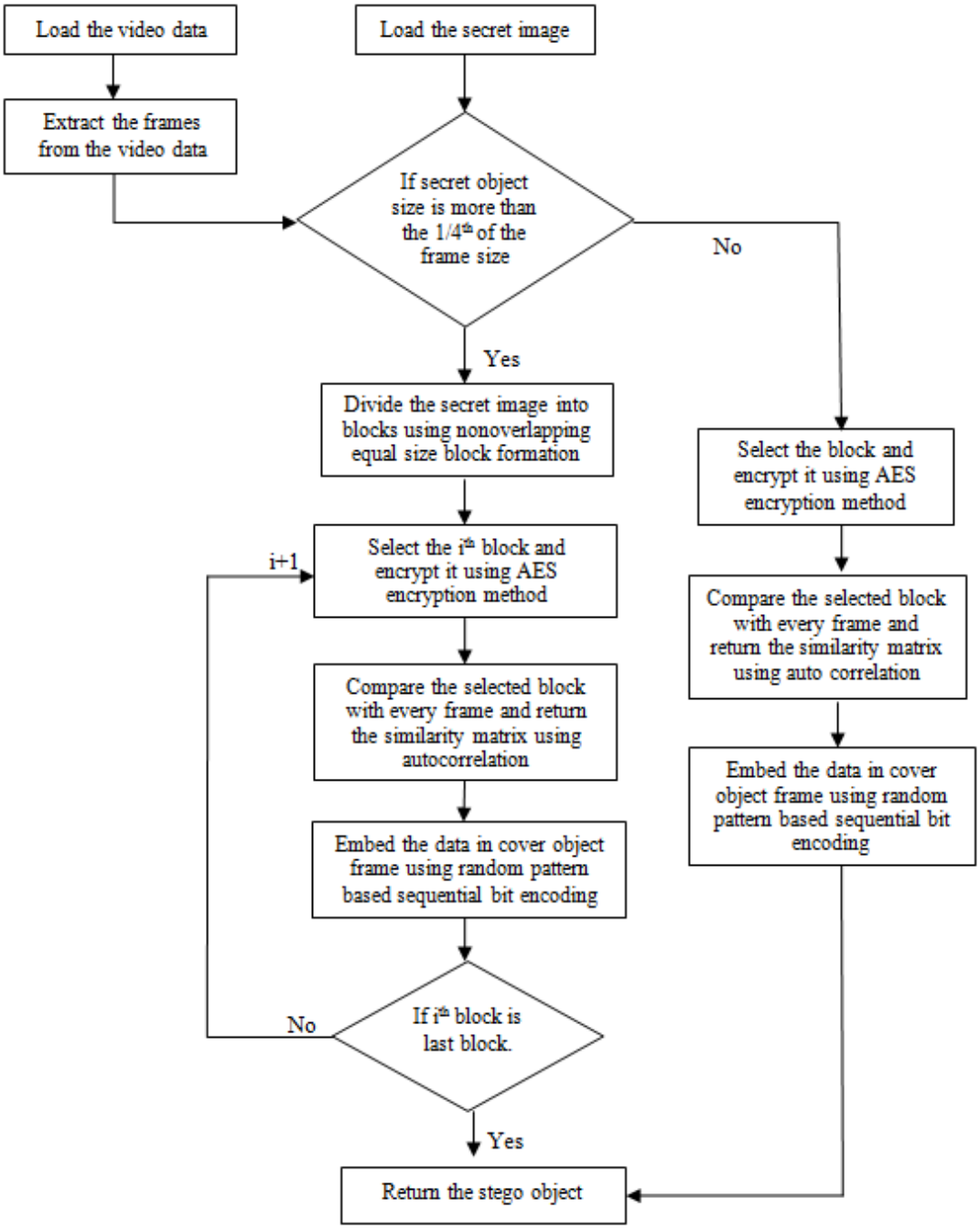

Fig.2. Workflow of the Proposed Model

5. Experimental Results

The results of the proposed model have been obtained in the form of chi-square histogram difference measurements. Two images have been tested under this test and the very less difference has been recorded between the input images. One image from the Professor Wang's database of 10000 images has been selected, which belongs to the tribal people group. The image distributes the variety of the colors in the tribal people photos, whereas the other photo is the standard image, which is called the Lena image. The Lena image defines the even distribution of the magenta color and shows the interruptions very clearly when the data is embedded in the image matrix. Even when the very little change is reported, the image matrix may change drastically in the visual as well as in the histogram difference.

Fig.3.The First Original and the Stego Image

The first original image is shown in figure 3, and this image contains the two tribal children with few people in the background. Also, the greenery has been seen in the background visuals of the given image. The proposed model embedding has shown no visual difference between the two image (original and stego object) during the embedding mechanism.

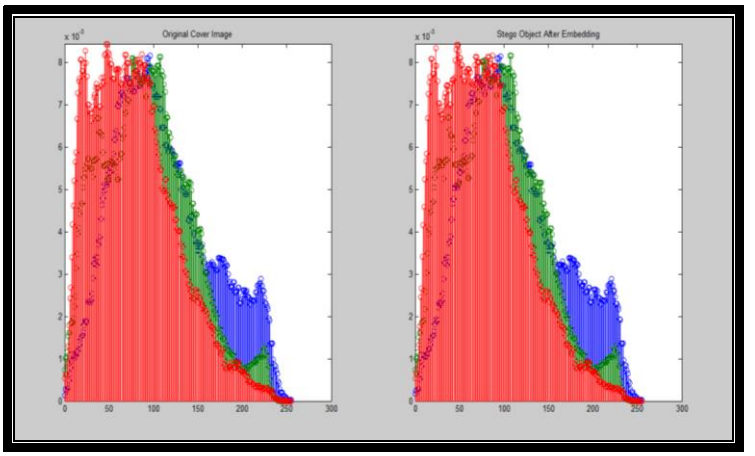

Fig.4.The Chi-Square Test over the First Stego Sample

The chi-squared error has been measured between the original and stego image collected from the Professor Wang's database of 10000 images. The proposed model embedding has shown very less difference between the two image as per shown from the histograms obtained from the original and stego image. The minimal error assures the robustness of the steganographic model in figure 4.

Fig.5.The Second Original and Stego Image

The second original image is shown in the fig. 5, and this image contains the picture of a lady called Lena, which shows the even distribution of the colors in the image matrix. A very small change can be easily spotted in this image, but the proposed model embedding process image showed the minimized difference between these images. The proposed model embedding has shown no visual difference between the two image (original and stego object) during the embedding mechanism when tested with the proposed model.

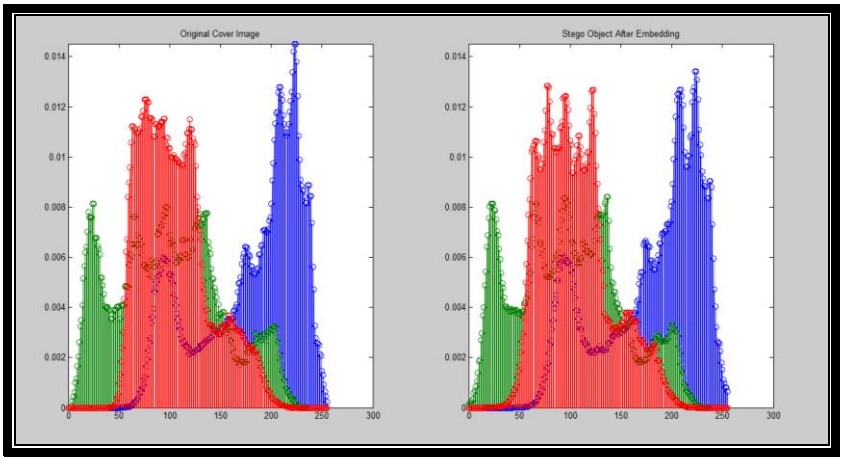

Fig.6.The Chi Square Test over the Second Stego Sample

The chi-squared error has been measured between the original and stego image collected from the standard Lena image. The proposed model embedding has shown very less difference between the two image as per shown from the histograms obtained from the original and stego image. The minimal error assures the robustness of the steganographic model in figure 6.

Table 1. The Squared Error Based Evaluation of the Proposed Model

Image Name	Squared Error
Lena	0.0062
Tribal	0.000461
Beach	0.0035
Urban	0.00015
Nature	0.0021

The above table shows the squared error values obtained between the original and stego image after applying the histogram based chi-squared error based evaluation. The maximum difference between 0.0062 and 0.000461 obtained from the squared error evaluation over the test case images. These values show the robustness of the proposed model in embedding the data in the image. This proves the high precision of the embedding using the low-bit steganography model based upon the pseudo random based embedding with the random shuffling pattern.

6. Conclusion

A technique for video steganography for secret transmission is proposed in this paper. The embedding of the covert data is done using the spatial and temporal techniques of the video signal. Various attacks on the steganography have been discussed. The proposed scheme is developed to ensure the more image security during transmission. This model is based on random rules in the cover image to increase the security for embedding the data. It gives an emphasis on the similarity between the cover and the secret object in order to find the most suitable matching region. On the other hand, if the similarity is not found, then it can adjourn the process of embedding. The proposed model is robust in nature wherein it accepts only those regions which are properly matched. The experimental results are obtained using the chi-square test over the images of Professor Wang's database. The purpose of this model is to increase security at a higher level.

References

[1] Mahajan, P., & Sachdeva, A. (2013). A study of Encryption algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*, *13*(15).

[2] Sherly, A. P., & Amritha, P. P. (2010). A compressed video steganography using TPVD. *International Journal of Database Management Systems (IJDMS) Vol*, *2*, 764-766.

[3] 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).

[4] Xu, C., Ping, X., & Zhang, T. (2006, August). Steganography in a compressed video stream. In *Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on* (Vol. 1, pp. 269-272). IEEE

[5] Shukla, C. P., & Chadha, M. R. S. (2014). A Survey of Steganography Technique, Attacks, and Applications. *International Journal of Advance Research in Computer Science and Software Engineering*, *2*.

[6] Varghese, B. B., & Haroon, R. P. Reversible Encrypted Data Hiding In Encrypted Video.

[7] Kelash, H. M., Abdel Wahab, O. F., Elshakankiry, O. A., & El-sayed, H. S. (2013, October). Hiding data in video sequences using steganography algorithms. In *ICT Convergence (ICTC), 2013 International Conference on*(pp. 353-358). IEEE.

[8] Thakare, M. S. S., & Bhale, N. L. A Review of Digital Image Steganography Techniques.

[9] 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

[10] 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.

[11] Hussain, M., & Hussain, M. (2013). A survey of image steganography techniques.

[12] Mandal, P. C. (2012). Modern Steganographic technique: A survey.*International Journal of Computer Science & Engineering Technology (IJCSET)*, *3*(9), 444-448.

[13] 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.

[14] Kour, J., & Verma, D. (2014). Steganography Techniques–A Review Paper.*International Journal of Emerging Research in Management &Technology ISSN*, 2278-9359.

[15] Ramalingam, M., & Isa, N. A. M. (2014, October). A steganography approach for sequential data encoding and decoding in video images. In *Computer, Control, Informatics and Its Applications (IC3INA), 2014 International Conference on* (pp. 120-125). IEEE.

[16] Kumar, M. S., & Latha, G. M. (2014). DCT Based Secret Image Hiding In Video Sequence. *Journal of Engineering Research and Applications www. ijera. com ISSN*, 2248-9622.

[17] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, *24*(9), 1613-1626.

[18] Sharma, M. H., MithleshArya, M., & Goyal, M. D. (2013). Secure Image Hiding Algorithm using Cryptography and Steganography‖. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, 2278-0661.

[19] Shakir, Ahmed C. "Stego Encrypted Message in Any Language for Network Communication Using Quadratic Method." *Journal of Computer Science* 6.3 (2010): 320.

[20] Divya, K. P., & Mahesh, K. Random Image Embedded in Videos using LSB Insertion Algorithm.

[21] 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).

[22] Yadollahpour, A., & Naimi, H. M. (2009). Attack on LSB steganography in color and grayscale images using autocorrelation coefficients. *European Journal of Scientific Research*, *31*(2), 172-183.

[23] Manibharathi, N., Krishnaprasad, S. (2014). Transform DomainTechnique in Image Steganography for Hiding Secret Information. International Journal of Engineering Research & Technology (IJERT), 3(2). pp. 1255-1260.

[24] Juneja, M., & Sandhu, P. S. (2013). A new approach for information security using an improved steganography technique. *Journal of Information Processing Systems*, *9*(3), 405-424.

[25] Singh, S., & Agarwal, G. (2010). Hiding image to a video: A new approach of LSB replacement. *International Journal of Engineering Science and Technology*, *2*(12), 6999-7003.

[26] Jain, Y. K., & Ahirwal, R. R. (2010), "A novel image steganography method with adaptive number of least significant bits modification based on private stego keys," International Journal of Computer Science and Security (IJCSS), *4*(1), pp. 40-49.

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.

How to cite this paper: Ravpreet Kaur, Manish Mahajan,"Random Pattern Standard Bit Embedding for Minimized Histogram Difference", International Journal of Education and Management Engineering(IJEME), Vol.7, No.1, pp.54-64, 2017.DOI: 10.5815/ijeme.2017.01.06