iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4252

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

A Method for Steganography using Edge Detection through Operator

Ms. Sanjukta Chakraborty[1], Prof. Samir Kumar Bandyopadhyay[2]
[1]*Seacom Skills University, India*
[2] *Department of Computer Science and Engineering, University of Calcutta, India*

Abstract: ***In recent times, privacy protection is a special stream of studies to evolve new methodologies to cope up with recent threats and malicious attacks. Steganography is a method of data hiding where cover object is used to hide secret data and generates a Stego object.***
Since Stego objects are look-a-like of cover object, it is not readily noticeable as a carrier of hidden data. The objectives of steganography are un-detectability, robustness and embedding capacity. A new technique of image steganography is proposed using the concept of edge detection. An operator with unique feature is selected to find maximum edge strength in different orientations.
Keywords: Digital Steganography, Image Steganography, Edge Detection, Operator Selection

I. INTRODUCTION

The basic model of Digital Steganography is composed of three types of objects: Cover or Carrier or vessel object, secret object and Stego object. In a simple manner, Cover plus Secret is equal to Stego. Depending on the type of the cover object there are different types of Digital Steganography like Image Steganography, Audio Steganography, Video Steganography and Text Steganography.
Steganography is a method of data hiding where cover object is used to hide secret data and outputs a Stego object. Since Stego objects are lookalike cover object, it is not readily noticeable as a carrier of hidden data. Even smart intruders also have to perform several steganalysis attacks to destroy the secret or require exact extraction mechanism to excerpt the secret. The method of detecting the existence of the secret communication is “steganalysis”.
The main objective of steganography is imperceptibility or undetectability which means no perceptual degradation in Stego object. In other words, there should not be any clue of data hiding in the Stego object. The next important objective is robustness. Robustness means ability to withstand adverse situations which encourages the evolution of techniques which can not be tampered through steganalysis attacks.
Steganography can be blind or non-blind and key based or keyless. Blind steganography doesn’t require original cover to extract the embedded secret whereas non-blind technique does. Key based steganography uses keys to embed data as well as extract data. These keys even shared with recipient for successful extraction. Therefore Kerckhoffs's principle of crypto system must be examined to assure the successfulness of the technique. Steganography can be mathematically defined as follows:

$$\text{Em: } CxMxK \rightarrow S \quad (1)$$

$$\text{Ex: } SxK \rightarrow M \quad (2)$$

Where Em and Ex embedding and extraction mapping function, C is the cover object, K is the Key, M is the secret message and S is the Stego object.
The paper proposed edge based steganography along with analysis.This paper proposed a technique of image steganography using the concept of edge detection.
The novelty of this paper lies in the usage of Kirsch operator for image steganography. This operator has unique feature to find maximum edge strength in different orientations. Depending on a threshold value for the Kirsch operator and the intensity value of each pixel of cover image, a scale with 3 ranges would be created. This scale is the basis for choosing flexible i.e. 2, 3 or 4 LSB replacements for steganographic encoding. The threshold value is sharable to intended receiver as a key and if appropriate reverse approach is taken, cover image can be successfully retrieved. This work has been carried on different grey scale images, maximum payload has been calculated, Peak Signal to Noise Ratio(PSNR) and Structural Similarity Index(SSIM) values are compared to get satisfaction of aims of image steganography.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

II. LITERATURES REVIEW

The word “Steganography” is a Greek word, originated from steganos which means "covered, concealed, or protected," and graphy , came from greek word, means "writing". When a rectangular piece of paper with holes applied to a sheet of paper leaves open only some of its parts. This opened parts are composition of secret message. The intended recipient of the communication should have the same grille [1-2]. This method has been depicted in Figure 1(a). The microdot and microdot camera has been shown in Figure 1(b) and Figure (c).

Figure 1 (a) Cardan Grille (b) Microdots (c)Microdot Camera

Nazi, a German spy, invented few methods of steganography like microdots, invisible inks and null ciphers during World War II. The microdot is a photographic image reduced to the size of the period at the end of this sentence that can contain an entire page of typewritten text with perfect clarity. He used it to secretly transmit information through common postal channels. Another technique was using urine as invisible ink. Actually, Nazi spy used to hide his secret message in handkerchief using Copper Sulphate which can be revealed by Ammonia fumes. The third technique is null cipher. A null cipher is an ancient form of steganography where the plaintext is mixed with secret text. Therefore the cipher text/ stego text cannot be distinguished as a carrier.

In 1980 Margaret Thatcher, the former British Prime Minister, used a method of linguistic steganography by programming a word processor to encode identity of disloyal ministers of her cabinet in the word spacing of documents, so that they could be traced [3].

In present steganography became digital. It can be performed by digital objects like text, image, audio and video. The most traditional approach in digital steganography is Least Significant Bit Substitution technique. Text steganography can be performed by Line shift coding, Word shifting coding, Syntactic methods, Semantic methods and Feature coding. The steganography for image , audio and video can be broadly classified into spatial and frequency domain techniques. Spatial domain means normal image space. Therefore pixel positions are directly modified. For image steganography, most common spatial domain techniques are LSB substitution, Pixel Value Differencing, Grey level modification, Palette based and Parity checking[4]. For audio steganography, most common spatial domain techniques are LSB substitution and echo hiding method [5]. For video steganography, all the spatial domain techniques of image steganography are applicable [6]. The frequency domain analysis is analysing a signal with respect to frequency. In case of image, frequency means the rate at which the pixel values are changing in spatial domain. Image, Audio and Video can be transformed to frequency domain using DCT and DWT. Therefore DCT and DWT based methods are popular for Image, Audio and Video Steganography [7].

The steganographic framework can be better explained with the prisoner’s problem[8]. In 1984 G.J. Simmons stated a problem of communication between two prisoner named Alice and Bob. Whenever Alice and Bob required to communicate they have to use public channel which was closely monitored by warden, Wendy. Wendy used to punish both if subliminal communication is detected. Alice wants to sends a secret message S to Bob. By hiding it in a carrier message C, she obtains Stego signal x. Alice then send this x to Bob through public channel.

The most popular technique of steganography is Least Significant Bit (LSB) modification technique. This LSB technique has been also utilized in video steganography by different approaches. Researchers described a hash-based technique of LSB which is popularly abbreviated as HLSB technique [9]. Other researchers have described that the hash function can be used to find out LSB position where the secret data will be stored [10].

Researchers also used Local Binary pattern (LBP) to embed secret message in the chosen cluster of cover frame of the video [11]. The fundamental idea of LBP is to sum up the local structure in an image by comparing each pixel with its neighbourhood. For this

purpose, authors have first created cluster of cover frame. Clustering is a method of partitioning group of data points into a small number of clusters. This has been done by k-means clustering algorithm. It is an unsupervised learning algorithm specifically used in data mining and machine learning purposes. The first step of this algorithm is to determine the number of cluster k and assume the centroid of these clusters. Then in the next step determine the distance of each object from the centroid. At the final step, one need to group the objects based on minimum distance.

In recent years researchers proposed a joint approach (JA) for video steganography using irreversible and reversible methods [12]. In irreversible methods of data hiding original cover is unavailable once data hiding is done whereas in reversible method cover can be recovered from the stego after extracting the secret message. Others have embedded a video inside a video using linked list method [13]. The linked list method is used by embedding the byte of information inside one 3*3pixel, the address of the location of next byte of information should be embedded next to it. Recent research proposed EMD – Exploiting Modification Direction to propose a new technique of embedding namely Improved Matrix Embedding (IME) [14]. Some researchers embedded secret through traditional LSB approach but frame selection is done through a novel approach of entropy evaluation [15]. Entropy is evaluated by following equation:

$$E = -\sum_{i=1}^{GL} P(i)\log_2\left(P(d_i)\right) \quad (3)$$

Where, GL is gray level of the frame, P (d) is the probability of existence of gray level.

Researchers also identified N high entropy valued frame and split the secret in N parts. After that data embedding is done. Song, G., et al. (2014) have discussed a new technique of data hiding in video to reduce distortion drift using Multi-view coding video [16]. Multi-view coding video is a video compression standard that includes efficient encoding.

Recently researchers have used neighbouring similarity method for video steganography [17]. First the frames are generated then the histograms of those frames are drawn, and peak point is identified. From original frames prediction error is calculated. By using peak point and prediction error secret message is embedded in the specific frame. Hu, S. D., & U, K. T. (2011) have used a non-uniform rectangular portioning algorithm to embed a secret video of same size into a cover video [18]. Some researchers has proposed a compressed video secure steganography (CVSS) technique where secret data is embedded in the DC coefficient of the scene change point [19].

Steganography is primeval form of invisible communication. With the advent of technologies, different digital objects like image, audio, text and video are used in Steganography [20]. A digital image is a collection of unitary element called picture element, in short pixels. A digital image can be represented as composition of binary bits. It has been seen that there are certain bits which are redundant in a manner that doesn't introduce any visual artefact in the stego image. Depending on modification in redundant bits the image steganography can be broadly implemented in three types of effective way like LSB Substitution, Blocking, and Palette Modification. LSB (Least Significant Bit) Substitution is the process of modifying the least significant bit of the pixels of the vessel image. Blocking works by breaking up an image into "blocks" and using Discrete Cosine Transforms (DCT) or Discrete Wavelet Transform (DWT).

III. PROPOSED METHOD

In this paper basic inputs for embedding procedure are as follows:

A. Cover image: Any Gray scale image
B. Threshold value: Range between 0-255
C. Secret message: Any text message, here messages from a 65KB sized text file has been chosen as secret message

Output of embedding procedure: Stego image – Gray scale image

Initially a threshold value T and pixel gradient P of Gray Scale are compared to separate edge Pixels from non edge Pixels. In this paper 8 directions of Krisch operators are used for the detection of edge in the cover image.

$$H_0^k = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad H_1^k = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad H_2^k = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

$$H_3^k = \begin{bmatrix} 0 & 1 & 1 \\ -1 & 0 & 1 \\ -1 & -1 & 0 \end{bmatrix} \quad H_4^k = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix} \quad H_5^k = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & -1 \end{bmatrix}$$

$$H_6^k = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix} \qquad H_7^k = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0 & -1 \\ 1 & 1 & 0 \end{bmatrix}$$

By using Kirsch operator, the edge magnitude is calculated as maximum magnitude in all 8 directions using the below kernel:

$$\|c_{m,n}\| = \max_{i=1,2,..8}(C_i) \quad (4)$$

where, $\|c_{m,n}\|$ is the edge magnitude, i is the Kirsch direction and

C_i is the response of the kernel at the pixel position i

$$C_i = \sum_{p=-1}^{1} \sum_{q=-1}^{1} H_i^k f_{m+p,n+q} \quad (5)$$

After getting the pixel values, Kirsch operator is used to detect edge image from the given image. This edge image would be used to embed secret data.

Each pixel of a grayscale image composed of a byte i.e. 8 bits. So, a pixel can have values between (2^0 -1) to (2^8 -1) i.e. 0 to 255. If the threshold value is 'T' then a scale of three ranges can be created by equation (6).

$$R = (255-T)/3 \quad (6)$$

Leaving first T values, a scale can be created as shown in equation (7 to 9):

$$R1 = (T \text{ to } T+R) \quad (7)$$

$$R2 = (T+R+1 \text{ to } T+2R+1) \quad (8)$$

$$R3 = (T+2R+2 \text{ to } T+3R+2) \quad (9)$$

The flexible type of LSB method would be chosen by Table 1.

Table 1 Mapping between Regions and LSB Method

Pixels in Region	Flexible LSB
R1	2-bit LSB
R2	3-bit LSB
R3	4-bit LSB

Now a calculation shall be done to check what would be the safe length to encode using this cover image. If the number of edges in the image is 'E' and each edge having average 'I' pixels in R1, 'J' pixels in R2 and 'K' pixels in R3 then the encoded safe length ('SLen') can be calculated by equation (10).

$$SLen = E*(I*2+J*3+K*4) \quad (10)$$

Now the length of the secret text is denoted by 'SecLen'. if SecLen>SLen then "Steganography can't be performed"; otherwise "Steganography can be performed; During the extraction process of secret data retrieval, it has been assumed that the threshold value is shared with receiver end. So, receiver will apply analogous approach to detect edges and finds where 2, 3 or 4 bits of LSB substitution have been done. Depending on those information, secret image bytes can be rebuilt and thereafter complete secret image can be extracted.

The following figure 2 shows steps for embedding and extraction techniques.

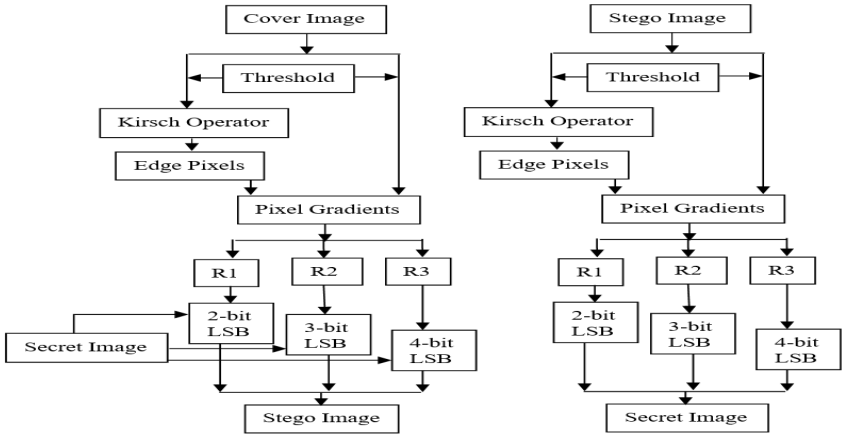


Figure 2 It shows embedding and extraction procedures

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

IV. RESULTS ANALYSIS

Table 2 illustrates the stego images which have been generated by applying different LSB methods using diversified threshold values. These stego images are visually similar to the cover image, hence they don't reveal the existence of secret embedded image anyway.

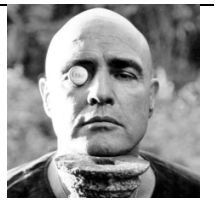
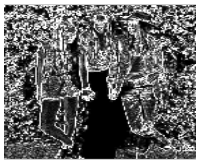
Cover Image	Edge Image by Key Operator	Stego Image
		
Dennis Hopper	Threshold =10	2-bit LSB
		
Sergio De Arrola	Threshold=100	3-bit LSB
		
Californian Girl	Threshold=200	4-bit LSB

Table 2 Creating Stego Images with Different Thresholds

Table 3 demonstrates the results of Quality metric for original secret vs. extracted secret.

Original Secret	Extracted Secret	Quality Results
		PSNR: 65.0172 SSIM: 0.9989
		PSNR: 73.8014 SSIM: 0.9849
		PSNR: 76.7042 SSIM: 0.9726

Table 3 Quality Analysis for the Original Secret vs. Extracted Secret Images

Bhattacharyya distance (D_B) can be used as a measure of detectability [21], which defines how much the Stego image reveals the existence of secret message. The D_B is measured between two discrete or continuous probability distributions Pd and Pc over the space Ω as shown in equation (11).

$$D_B(Pd, Pc) = -\ln \rho B(Pd, Pc) \quad (11)$$

$$\text{Where } \rho B(Pd, Pc) = \int_{\Omega}^{0} \sqrt{Pd(\omega)Pc(\omega)}d\omega$$

After calculation of D_B using equation 8 it needs to be normalized between 0 to 1 where 0 means full detectability and 1 means zero detectability.

Table 4 shows the quality of result analysis for one of the cover images. The outcome of PSNR and SSIM values demonstrate that the stego image is perceptually equivalent to the original image. The values of D_B are nearer to 1 signifies less detectability of this proposed method.

Threshold (T)	Safe Length (SLen)	Secret Length (SecLen)	PSNR	SSIM	D_B
10	74622	50	74.4487	1.000	0.9946
10	74622	20000	58.5316	0.9994	0.9970
10	74622	74622	39.5316	0.9729	0.9966
100	23423	50	69.3848	1.000	0.9970
100	23423	2000	53.9571	0.9995	0.9988
100	23423	23423	42.3665	0.9944	0.9946
200	12089	50	67.9071	1.000	0.9966
200	12089	5000	47.2873	0.9986	0.9970
200	12089	12089	42.9289	0.9964	0.9946

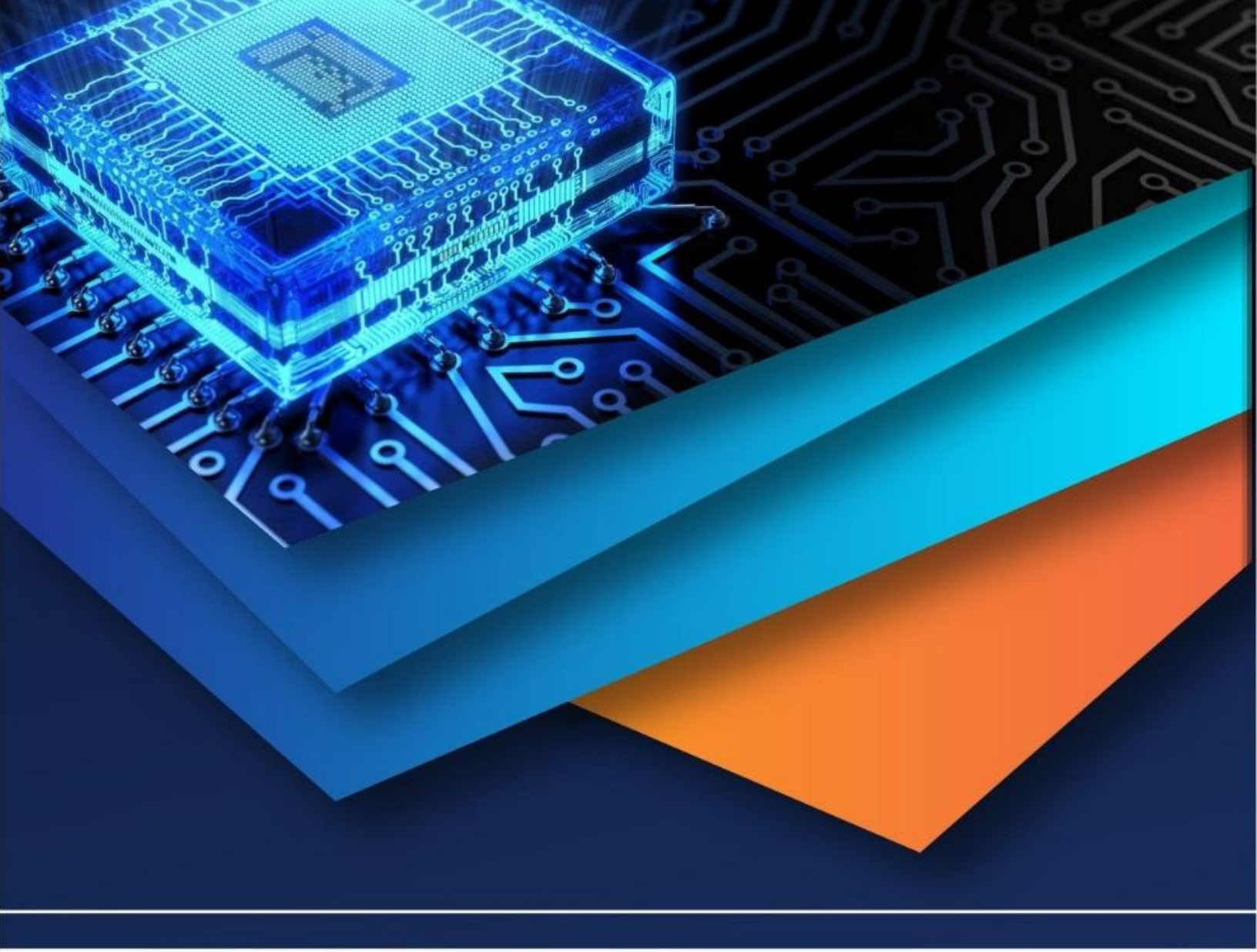
Table 4 Quality Result analysis for images of Dennis Hopper

V. CONCLUSIONS

Here image steganography using the concept of edge detection has been discussed. The use of key has unique feature to find maximum edge strength in different orientations. Depending on a threshold value and the intensity value of each pixel of cover image, a scale with 3 ranges is created. The results analysis shows that the method has better performance on different images.

REFERENCES

[1] J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker," Digital watermarking and steganography", Morgan Kaufmann, 2008.
[2] Utepbergenov, Irbulat, Janna Kuandykova, Tamerlan Mussin, and Sholpan Sagyndykova, "Creating a Program and Research a Cryptosystem on the Basis of Cardan Grille," IEEE, 2013.
[3] Judge, J.C, "Steganography: Past, Present, Future", SANS,2008.
[4] Shelke, S.G., and S.K. Jagtap, "Analysis of Spatial Domain Image Steganography Techniques," IEEE, 2015.
[5] Bilal, Ifra, Rajiv Kumar, Mahendra Singh Roj, and P K Mishra. "Recent Advancement in Audio Steganography," IEEE, 2014.
[6] Dalal M., Juneja M, "Video Steganography Techniques in Spatial Domain—A Survey", Lecture Notes in Networks and Systems, Springer, 2018.
[7] Kayem, Anne, and Christoph Meinel, "Information Security in Diverse Computing Environments: Advances in Information Security, Privacy, and Ethics", IGI Global, 2014.
[8] Li, Chang-Tsun, "Multimedia Forensics and Security", Information Science Reference, 2009.
[9] Deshmukh P. R., Rahangdale B, "Hash Based Least Significant Bit Technique for Video Steganography", Int. Journal of Engineering Research and Applications, 2014.
[10] Riasat, R., Bajwa, I. S., & Ali, M. Z, "A hash-based approach for colour image steganography", IEEE, 2011.
[11] Singh, D; Kanwal N, "Dynamic video steganography using LBP on CIELAB based K-means clustering", International Conference on Computing for Sustainable Global Development (INDIA Com), 2016.
[12] Umadevi R," Joint Approach for Secure Communication Using Video Steganography", 3rd International Conference on Computing for Sustainable Global Development (INDIA Com), 2016.
[13] Selvigrija, P., & Ramya, E. "Dual steganography for hiding text in video by linked list method", IEEE, 2015.
[14] Qian, L., Li, Z., Zhou, P., & Chen, J, "An Improved Matrix Encoding Steganography Algorithm Based on H.264 Video", IEEE, 2016.
[15] Seema, & Chaudhary, J. (2014). A Multi Phase Model to Improve Video Steganography (pp. 725–729). IEEE, 2014.
[16] Song, G., Li, Z., Zhao, J., Tu, H., & Cheng, J, "A video steganography algorithm for MVC without distortion drift" IEEE, 2014.
[17] Firmansyah, D. M., & Ahmad, T, "An improved neighbouring similarity method for video steganography", IEEE, 2016.
[18] Hu, S. D., & U, K. T, "A Novel Video Steganography Based on Non-Uniform Rectangular Partition", IEEE,2011.
[19] Liu, B., Liu, F., Yang, C., & Sun, Y," Secure Steganography in Compressed Video Bit streams", IEEE,2008.
[20] Mishra R and Bhanodiya P, "A Review on Steganography and Cryptography", IEEE International Conference on Advances in Computer Engineering and Applications, 2015.
[21] Geetha C.R, Basavaraju S, Puttamadappa C, "Variable Load Image Steganography using Multiple Edge Detection and Minimum Error Replacement Method", IEEE, 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY