Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 4190-4201*

Research Article

An approach for Secured Image Transmission: A High Capacitive and Confidentiality based Image Steganography using Private Stego-Key

G.Aparna[a], M.Kezia Joseph[b], C.N.Sujatha[c], Mankala Narender[d], Dr. B.RAJENDRA NAIK[e]

[a]Research Scholar, Department of Electronics and Communication Engineering, University College of Engineering, Osmania University-500040, Telangana, India
[b] Professor, Department of ECE ,Stanley College of Engineering& Technology for Women , Nampally, Hyderabad, India
[c] Professor,Department of ECE, Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India
[d] Lecturer in EIE Department, Government polytechnic, Kothagudem,Telangana, India.
[e] Professor and Head of the Dept., Dept. of Electronics and Communication Engineering, University College of Engineering (A), Osmania University. Hyderabad-500007, Telangana State

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: In the proposed paper an approach for image transmission with security and also improvement of the gray-scale (8-bit image) image flexible stenographic system using LSB approach. In this process a secret key of 80 bits is applied while embedding the message into the cover image. To provide high security and also confidentiality of the data a key stego-key is applied. The proposed method the information bits are embedded adaptively into the cover-image pixels. With this method a high embedding capacity in terms of hiding the data is provided and also better imperceptibility is also achieved. The major advantage of this method verifies by the Security method of Digital Signature. It is to be verified whether the attacker has made a trials to change the Secret information in the present inside the stego-image which is intended to be kept secret throughout the communication process. In this technique the embedding process to hide the message data present in the transformed spatial domain of the cover image and makes use of a simple Exclusive-OR operation based on Security checking method of verifying the signature digitally by using key size value of 140 bits is used to check the integrity from the stego-image. The confidential data which is embedded can be retrieved from stego-images. The security level is enhanced by using the stego key and by adaptive steganography data inconspicuousness is improved..

Keywords: Steganography, stego-image, cover-image, LSB-Least Significant Bit, digital signature, stego-key, security, data hiding, and digital image

1. Introduction

Information security, authentication, confidentiality and data integrity are the major requirements in network security and data communications so as to shield the data against illegal user access in the process of various wireless and multimedia applications [6],[7] of digital information. This has initiated for rapid growth in the field of data hiding. Existing literature of information protection the data hiding techniques are used comprehensively to list a few in areas like defense, medical, digital forensic, health care applications. To defend secret information from being misused during transmission, this challenging situation can be handled in two ways. Initially the encryption process is done in which the information that is to be kept secret is converted in to unintelligible form so that unauthorized users cannot access the data unless and until they have the correct key. Second way is steganography, this is taken from the Greek word meaning enclosed inscription this is of two types basically modification and substitution methods. In the proposed approach substitution method is employed. The main objective is secret communication process hiding the data. In the steganography the basic terms like cover image, stego-key, explains the original information message, data, audio, still video modes of input data. If the cover image of a particular size of digital image which is considered to be concealed with secret information, this representation is identified as stego-image. Steganography protects the secret message with the host data set and its existence is imperceptible. The paper is structured with research motivation in section 2, basic terminology of steganography in section 3, section 4 proposed techniques, followed by results discussion in section 5 and conclusion remarks with the future scope in section 6 and 7 respectively.

2. Research Motivation

In the process of image transmission an approach for secured and improved capacity for multimedia applications is proposed. The revolution in information security era the data is to be secured from unauthorized users accessing the data [1]. This is possible with the simple Least Significant Bit (LSB) substitution method of steganography. Using stego analysis to discover and remove hidden files manipulations are possible due to

which security has become a challenge, hence to handle this situation strong stego-key is used which further provides confidentiality as well by using private key.

3. Basic Terminology of Steganography

Image steganography is commonly preferred media because it is secured and confidential as well. Image steganography can be established, based on the operational area and the transformation type namely spatial domain and frequency domain. In Image steganograph method will modify the image pixel value directly and change the image gray pixel value. In the frequency domain transformation method the images are initially converted in to the frequency domain and then information is embedded in the transformed co-efficients .The process of Steganography is basically categorized as symmetric and asymmetric. In general, steganography process performs the evaluation of the equation defined as stego medium implies cover medium added with secret message and stego key. The stego key plays a vital role to control the data hiding process. The basic terms in the steganography model include the definitions of cover image, stego-image, perceptibility, robustness and security. The cover image is the distinctive representation in which the hiding data is to be embedded . In this process there should not be any distortion while embedding the information. The image obtained after embedding is identified as stego-image. Perceptibility is represented as detecting the presence of the information hidden in the image steganography. It should not be making out by the unintended user at the other end. Robustness is the characteristic indicating the strength against during embedding and extraction process

4. Proposed Technique

The process of implementing the proposed method five steps are followed they are namely step1 is private stego-key generation step2 is technique that examines the range and number of bits to be appended, step3 is LSB Substitution[2]. step4 is pixel value adjusting method step 5 is digital signature. The scheme is to evaluate range of pixels which cover the image Stegnography and an flexible LSB substitution in pixels are employed as shown in Figure 1 below. It's to be noted that the bits selected to insert should not distort the image at all. In this regard, the variable bits in terms of K are inserted into LSB part of thegray pixel value, which in turn depends on the the private stego-key K1. private stego-key K1 is present in five levels of gray pixel value. The range of gray pixel value will vary from 0 to 255 .The identified key has five ranges of gray pixel and every pixel image will replace the various unchanged quantity of bits into least substantial part of the 8-bit gray value of the pixels. After deciding the range of number of bits required to be inserted accordingly.

Pixel p(x, y) and the gray value "g" is present inside the examined limit value. Ai-Bi is transformed by embedded k information bits of secret data into new gray value "g". This new gray value is g prime (g^1) of the pixel may go beyond the range Ai-Bi. This is identified as over flow problem and it is a challenge to retrieve the exact information without any loss at the receiver end. Precise gray value modification method is used to update the current values within the examined limits Ai-Bi.

In process of fulfilling the networking and data communication properties like Confidentiality, Integrity and Digital Signature this following steps are followed. The confidentiality property is provided by the secret image steganography key and to afford integrity of the embedded unseen hiding data, 140-bit another key K2 is used. Digital signature of embedding the unseen hiding the data by using the secret key .

5. Private stego-key generation

In the private stego-key generation process for the input gray scale images 8 bits are represented to denote the pixel value intensity, so there are only 256 gray values at the most can be hold. Various pixels in the input pixel data may have a variety of gray values. The picture elements of images are divided into diverse categories depending on the gray value limits.

6. Method to decide number of Bits insertion into each range.

From the proposed method figure the number of bits required to insert are intended. In this process, now take into account of five gray levels values obtained by the image steganography key are identified as { A1-B1, A2-B2, A3-B3, A4-B4, and A5-B5} and arithmetical count & computation from cover image in each five levels values ranging from {N1- N5}. Next calculate the quantity of pixel in every level the cipher of digital values placing is fixed in the complete process. Similarly the bits required for extraction process is decided from the image steganography.

7. LSB Substitution.

An adaptive LSB substitution method is implemented in the projected proposal scheme of flexible K-bits of secret data are placed in Least significant part of image pixel value . Figure 2 depicts the complete procedure for K bits insertion. LSB substitution is most commonly used method for spatial domain. The LSB of a randomly

chosen building block is transformed to hide the data. This is simple and easy to implement. The quality of the host image is reserved. It assures high perceptual transparency.

8. Pixel value adjusting method

In the process of image elements pixel value regulation method, overflow of bits may be possible after combining the K information data bits into the gray pixel value 'g' will become new gray pixel value g'. To understand this, consider as an example the key range is 0-32. Consider for example the input initial value is $(00100000)_2$. Decided K-bits insertion is 3 and is denoted as $(111)_2$.The updated 'g' will be after inclusion is $(00100111)_2 = (39)_{10}$. Modified value is observed to be in over flow condition. To adjust among 0-32, K+1 bits of g' is flipped from logic 0 to logic 1 and vice versa. And recheck the evaluated level values else K+2 bit is modified and until attaining the gray value descend inside level. The complete process of pixel value adjusting method is given in Figure 3.

9. Digital signature

For verifying the integrity of the steganography image and hidden data, A normal EX-OR technique to discover the digital signature of secret data with random steganography-key size of 140 bits are used and joined with the message, some outgoings occurs but integrity of the message data is verified at the receiver side. Digital signatures are valid to prove the certification of the message generated by a particular individual. It also provides the information of the message generated individual assuring that the information has not been modified by any means [13]. Digital Signature offers an added advantage over secret key based cryptographic MAC's is non-repudiation. Digital signature function includes the authentication function.

In this context there is a vast scope of Elliptic Curve Cryptography with Secured Has Algorithm (SHA) has wide range of application in biometric especially [4]. In this regard a digital signature function should have the properties and requirements like the signature must be a pattern that depends on the message being signed, the signature must be some unique information to be conveyed to the sender to protect both the forgery and denial of the signature, it must be easy to produce and prove the identity whenever and wherever required, it must be computationally infeasible to forge by a fraudulent digital signature for a given message, finally it must be practical to retain a copy of the signature in storage, where compact storage also play a vital role to store in the data base.

10. Message Extraction Process

The block diagram in Figure 4 drawn below depicts the message extraction process flow. This is the turn round process of the data implant to regain the original data from the steganography image. In this process of extraction the algorithm chosen to implant and extract should assure the robustness of the information intended to transmit and also there should not be any loss of information while regain the data.

11. Algorithm for Embedding

Input: input cover-image, secret information to be hidden, K1, K2are the keys respectively

Output image: Stego-image**.**

Step1: gray-Level value limits are Examined and read the key K1 initially

Step2: Reading the cover image which is of 8bits gray type or of 8 bits colour image blue channel

Step3: calculate the number of bits required to insert into each range.

Step4: bit stream conversion process after reading the secret message.

Step5: Next examine the second key K2.

Step 6: Evaluate the digital signature using the key K2 and append information bits.

Step 7: In every picture element the gray value g, the K bits required to insert depending on the gray ranges in step2 and the new gray value g' are to be calculated thoroughly till the process is completed.

Step 8: End

Algorithm: Decoding

The Stego-image is given as input for decoding along with the keys K1, K2 respectively.

Resultant Output: the hidden message;

Step 1: Reading the keys K1 based on gray-level ranges considered in encoding.

Step 2: Reading the steganography image.

Step 3: Evaluate number of bits extraction in each and every range.

Step 4: For every pixel, retrieve the K-bits and accumulate the values.

Follow the steps performed in embedding process in the reverse way to decode exactly.

Step 5: convert the second key K2 and obtain the signature of digital data stream generated

Step6: Look for the signature obtained is matching or not.

Step 7: End

Figures 5 and 6 represent the flow diagrams of the message embedding with signature and extracting the signature process respectively.

12. Experimental Results and Comparative Analysis

In the implementation process of embedding and extracting of the proposed techniques the results are evaluated to show the skillful performance of the proposed approach in capacity and imperceptibility for hiding secret data in the stego-image [4], [5]. Different experiments are conducted using various images so as to compare with the proposed approach. The image of size 150X150 with 100% capacity using different stego-keys. It is observed from the tabulated results that this method can embed 20% more capacity than the method proposed earlier mentioned in the literature. The tables of the PSNR values list depicts that the performance is also improved compared to the existing approaches ensuring better security and enhanced confidentiality. To perform statistical analysis MSE and PSNR metrics are used which in turn denotes the quality of the image. In error analysis process the BER, MSE and PSNR play a vital role. MSE is calculated as the square of error between cover image and the stego-image. It is also measured as the distortion in the image. PSNR represents the ratio of the maximum signal to noise in the stego-image. The ratio is often considered as the quality measurement between the original image and stego image implying that the lower the value of MSE, the lower the error and the higher the PSNR, the better the quality of the output image. The formulas to calculate MSE and PSNR and mentioned below**.**

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

$$10\log_{10}\left(\frac{R^2}{MSE}\right)$$

Where, R denotes maximum fluctuation in the input image and for double precision R is1 and for 8-bit unsigned R is 255

13. Results Visualization

The images below shows the comparisions between original and stego of Lena and Pout respectively. Images visualization is shown in the form of images and in the Matlab simulation obtained figure12 and 14

14. Comparative Results

From the table 2 and the Figure 10 drawn for the tabulated values of the three methods it is observed that the proposed method is good in terms of capacity with the appreciable value of PSNR for the images taken as inputs for experimental investigation purpose.The Matlab simulation screenshots in Figure 11 denotes the Elapsed time of the message insertion of 220.016842 Sec, Figure 12 denotes Original image and stego image shown in the form of subplot, figure 13 denotes Message Extraction at the receiver of value 189.761071 Sec, Figure 14 denotes the Extraction of the original image

15. Conclusion

An steganographic approach is presented and an improved capacity to embed and as well as extract module based on the variable size LSB substitution is implemented. The stego-key is choosen within the gray value range between 0 to 255. The number chosen to adjust the method so as to minimize the embedding error and adaptive is 2 to 5 bits to embed in the picture elements to make best use of average capacity per pixel. With the proposed method message between 2 and 5 is embedded maintaining the imperceptibility. For security purpose different stego-keys can be used for different processing sessions.

16. Future Scope

The future scope includes the enhancement of the alogirthm to automatically select the number of bits insertion into pixel group selected using private stego-key that is based on gray-level ranges. Also a method for randomly

generating the stego-key by the system. A more advance scope for present multimedia applications is that the machine learning concepts can be used for statistical analysis so as to train and test the system for the same process and hence improve the performance further.

Table 1: Embedding capacity and image quality (PSNR) using different keys for different grayscale images.

	Grayscale images (8-bit)							
Different	Lena		Shadow		Baboon		Pout	
Stego-Keys	CAP	PSNR	CAP	PSNR	CAP	PSNR	CAP	PSNR
0-33,34-70,71-105, 106-170,171-255	2.99	39.5884	2.7118	42.6426	3.0389	43.0218	2.5141	44.156
2-35,37-73,74-105,106-170,171-255	2.9875	39.6058	2.7212	42.3987	3.0396	42.1201	2.5769	44.019
2-35,37-73,74-115,116-170,171-255	2.9497	39.4620	2.7204	42.4523	3.0336	42.2349	2.5960	43.505
0-45,47-85,86-143, 144-190,191-255	2.8573	41.3110	2.8438	42.0656	3.0229	41.7875	2.8220	41.682
0-45,47-85,86-143, 144-188,189-255	2.8667	41.1956	2.8372	42.2476	3.0208	41.8528	2.8222	41.778
Average values	2.9302	40.2325	2.7668	42.3613	3.0424	42.2196	2.6662	43.029

Table 2: The Comparative results of the embedding capacity (CAP) and image quality (PSNR) of proposed method with previous methods.

Grayscale	Embedding methods					
Images(8-bit)	Pixel value differencing		Tri-way PVD		Proposed method	
Size 150×150	CAP	PSNR	CAP	PSNR	CAP	PSNR
	Bits/pixel	(dB)	Bits/pixel	(dB)	Bits/pixel	(dB)
Lena	1.5551	41.79	2.3143	38.89	2.9302	40.2325
Shadow	-------	-------	-------	-------	2.7668	42.3643
Baboon	1.7178	37.90	2.5148	33.93	3.0424	42.2196
Pout	-------	-------	-------	-------	2.6662	43.0281

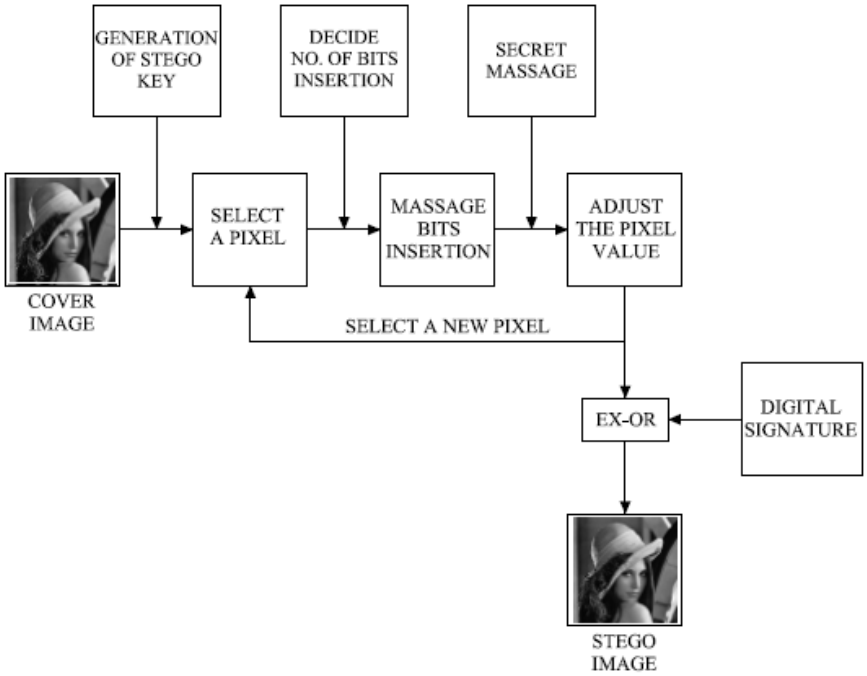

Figure 1: Block diagram for message Embedding

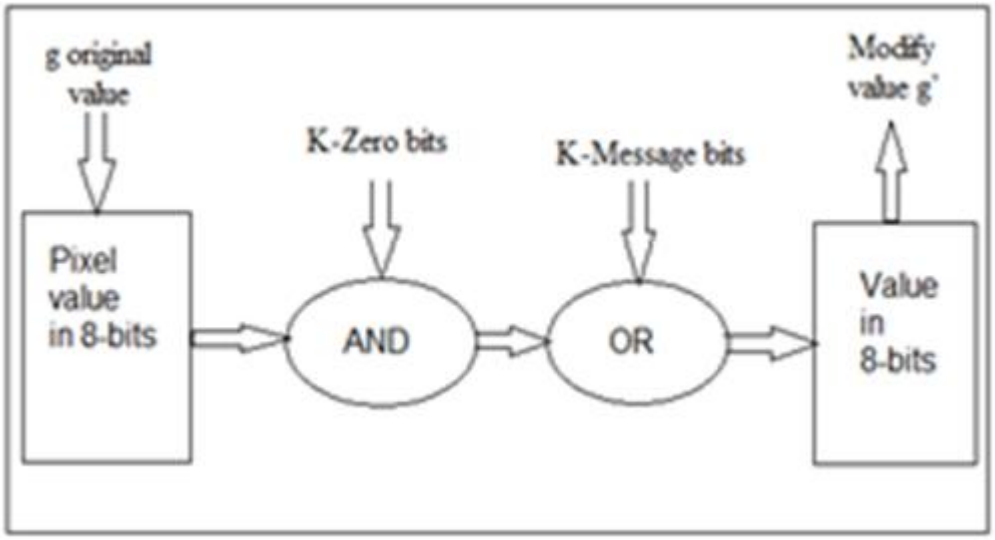

Figure 2: K bits insertion method representation

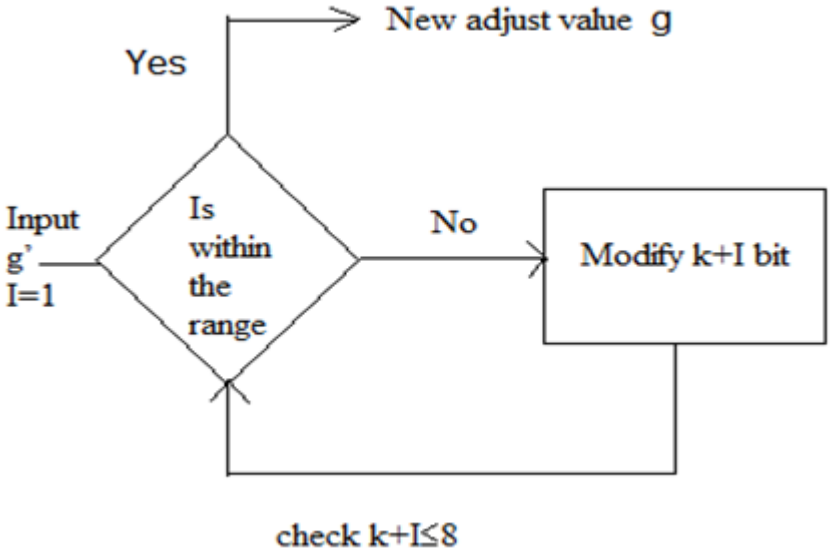

Figure 3: Pixel value adusting method

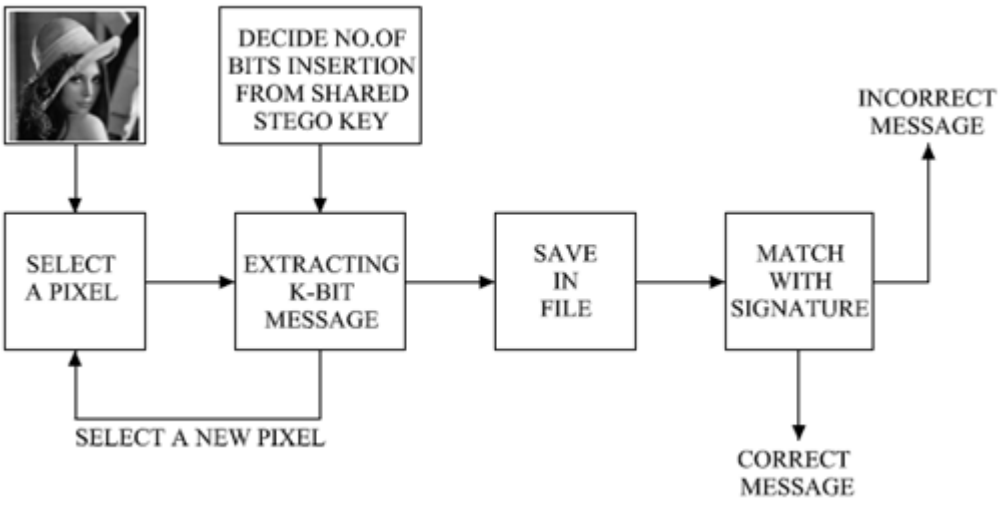

Figure 4: Block Diagram for Message Extraction and Integrity Check

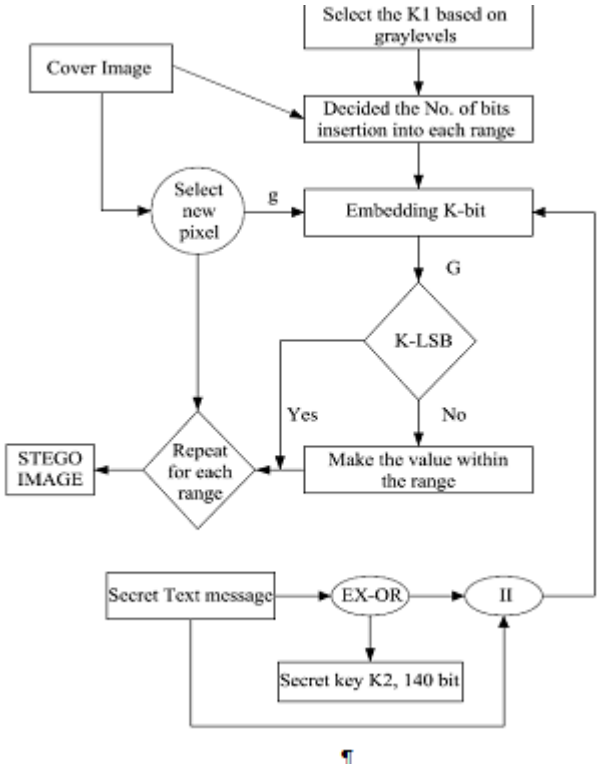

Figure 5: Flow chart for message embedding with signature

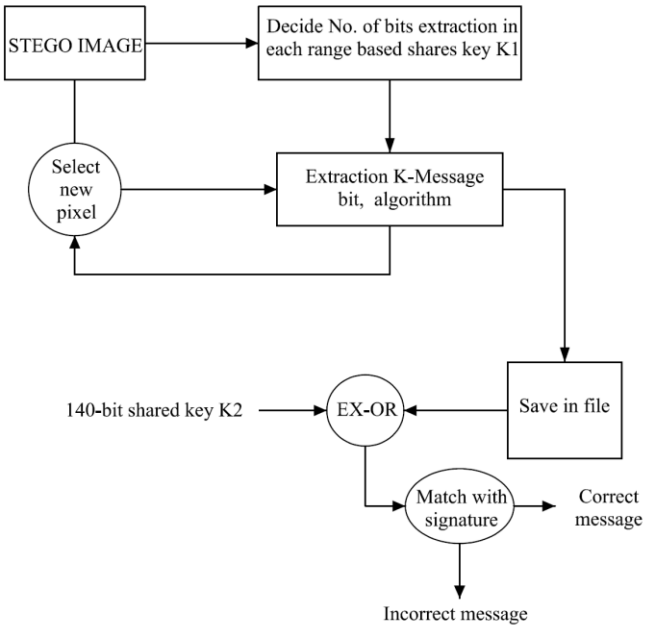

Figure 6: Flow chart message extraction and integrity check

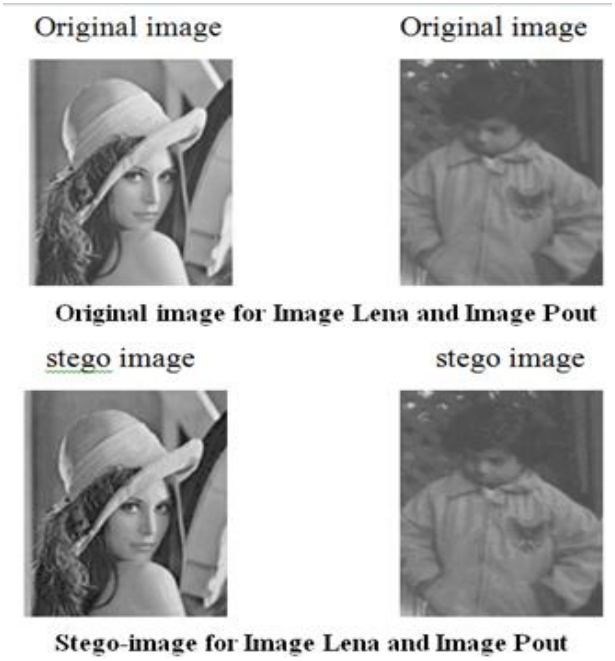

Figure7: Visualization of the original and stego image

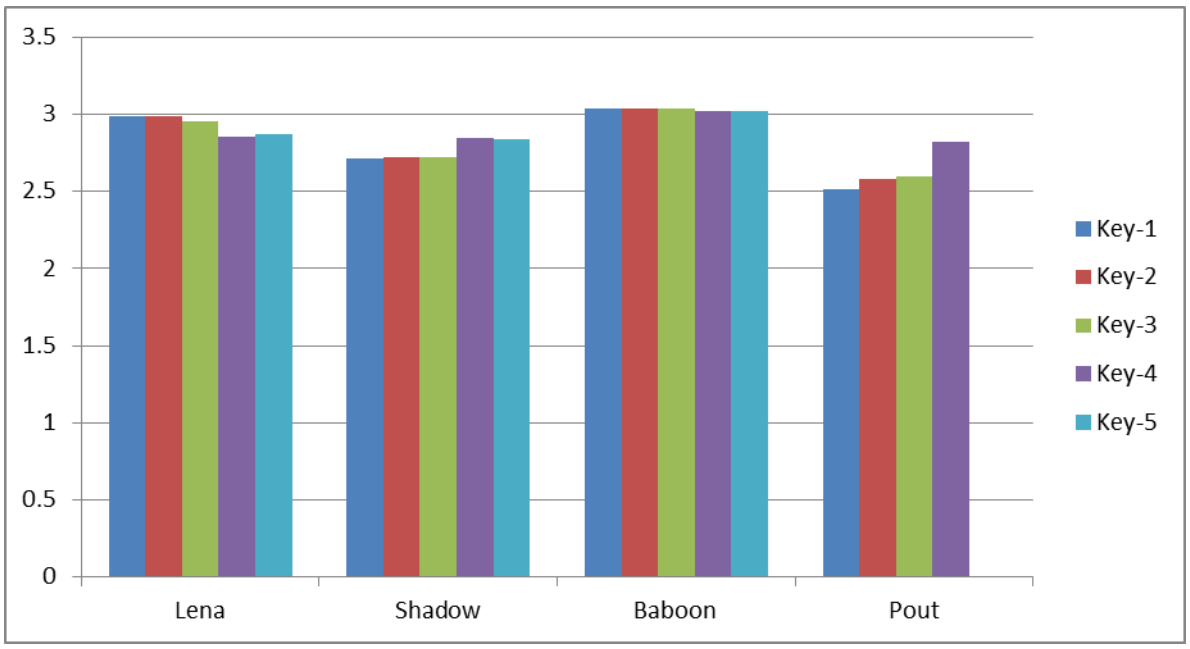

Figure 8: The graphical table of the results of table 1.

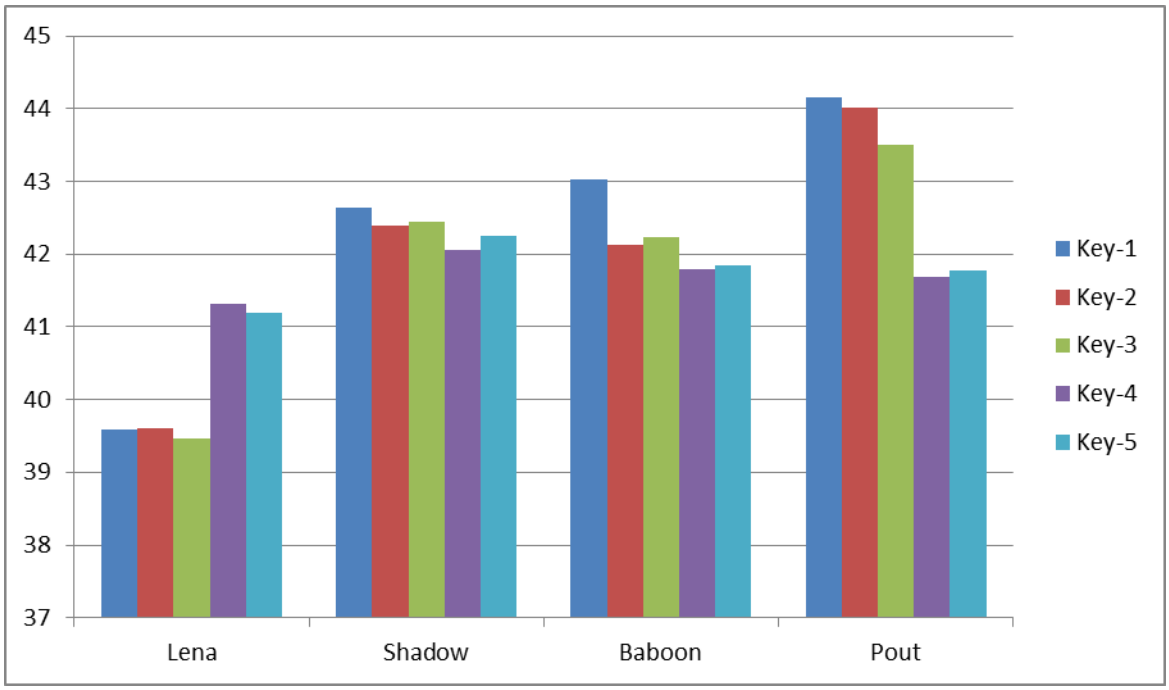

Figure 9: Graph of the PSNR using different stego-keys for different gray scale images.

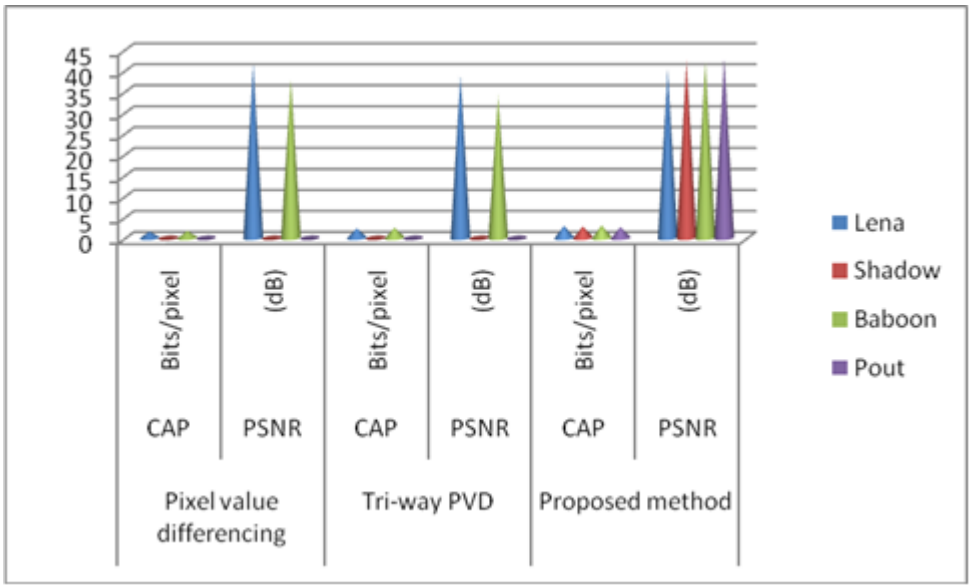

Figure 10: Graphical representation of the comparison table 2 for the embedding capacity (CAP) and image quality (PSNR) of proposed method with previous methods.

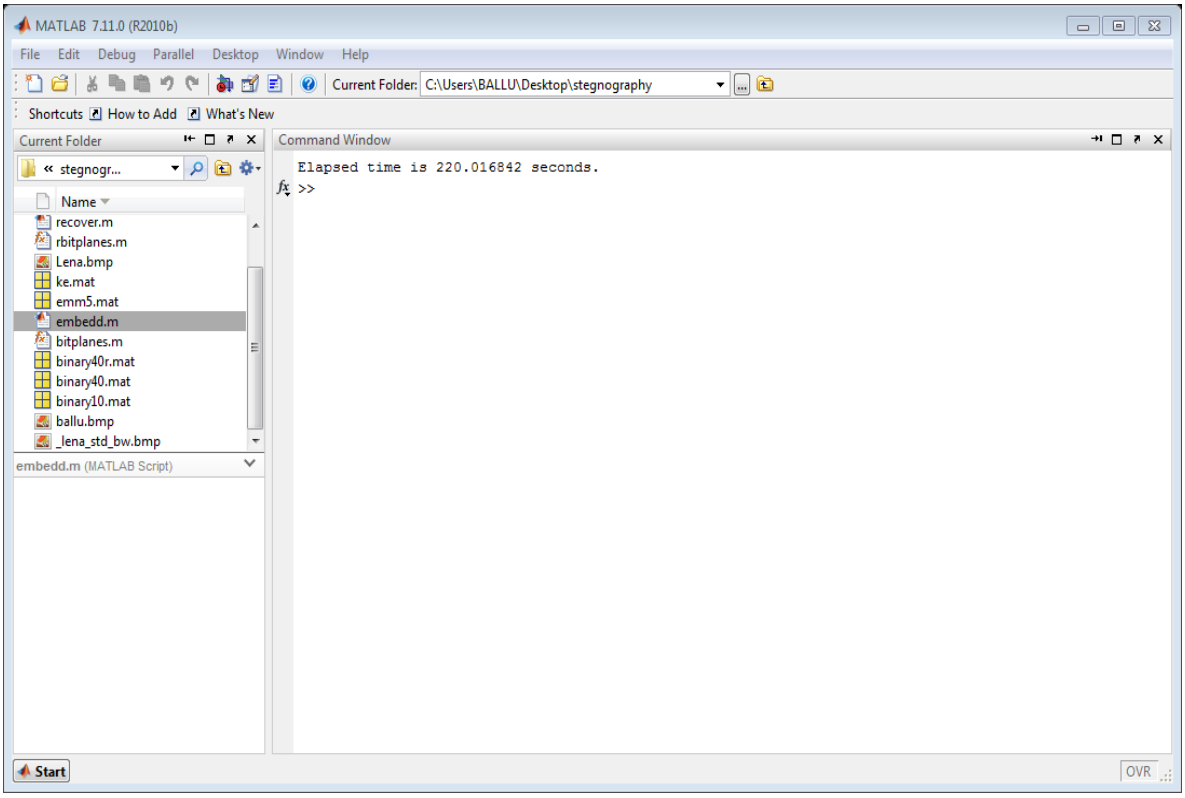

Figure 11: Elapsed time of the message insertion

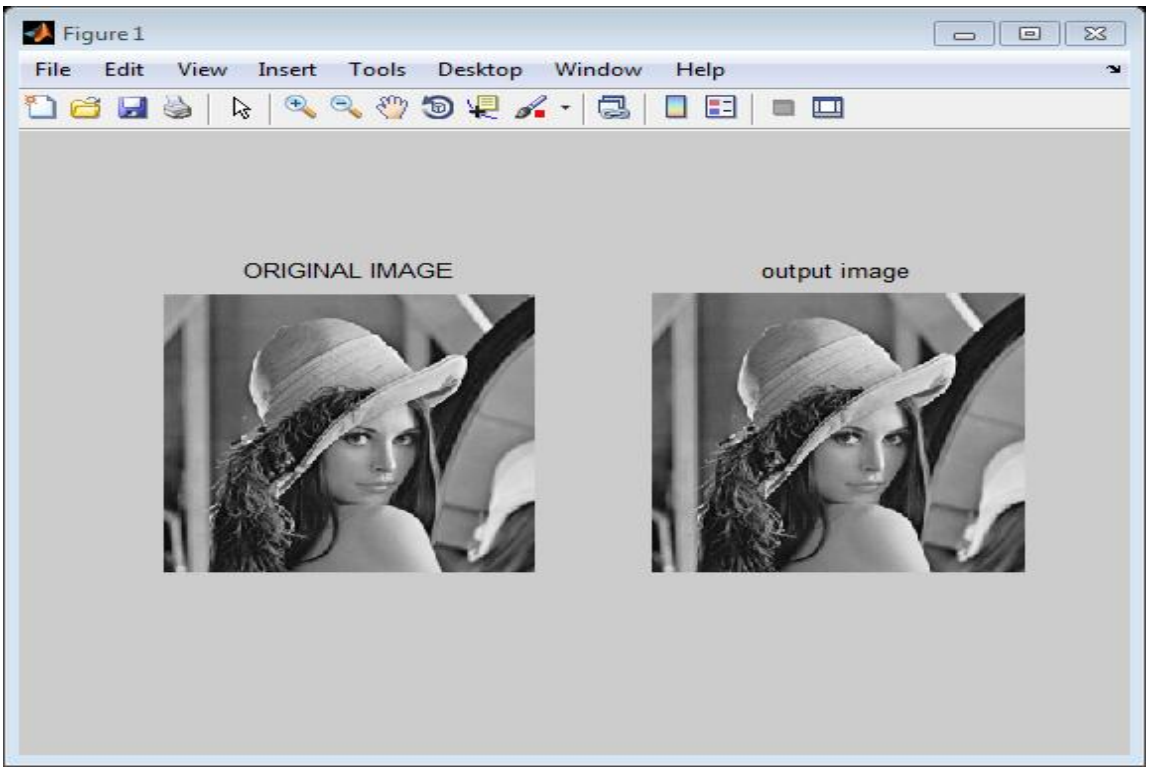

Figure 12: Original image and stego image

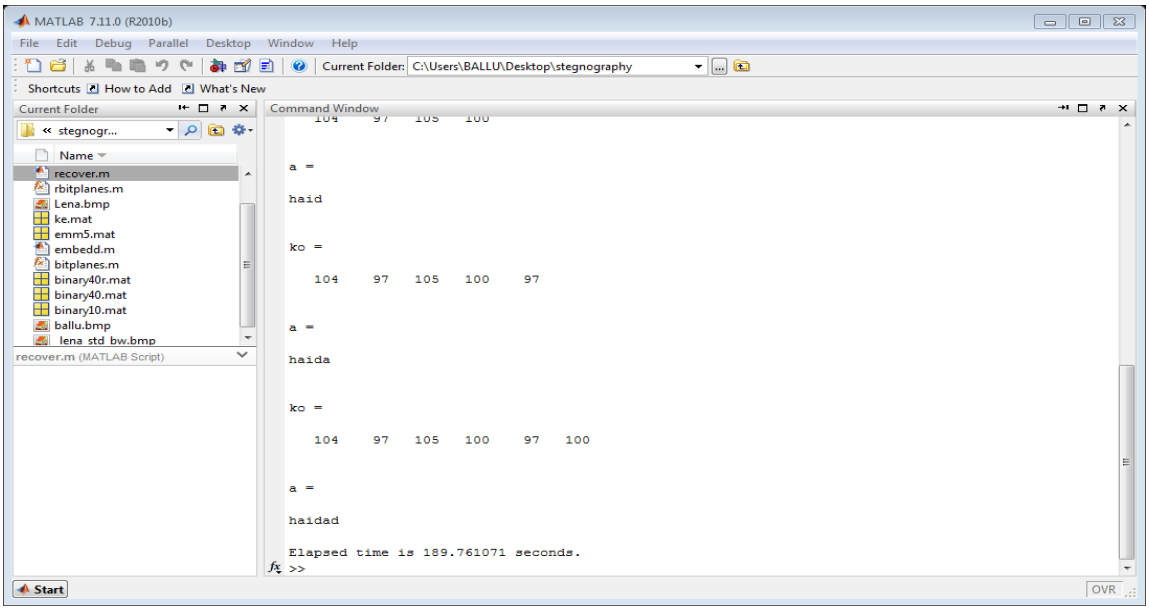

Figure 13: Message Extraction at the receiver

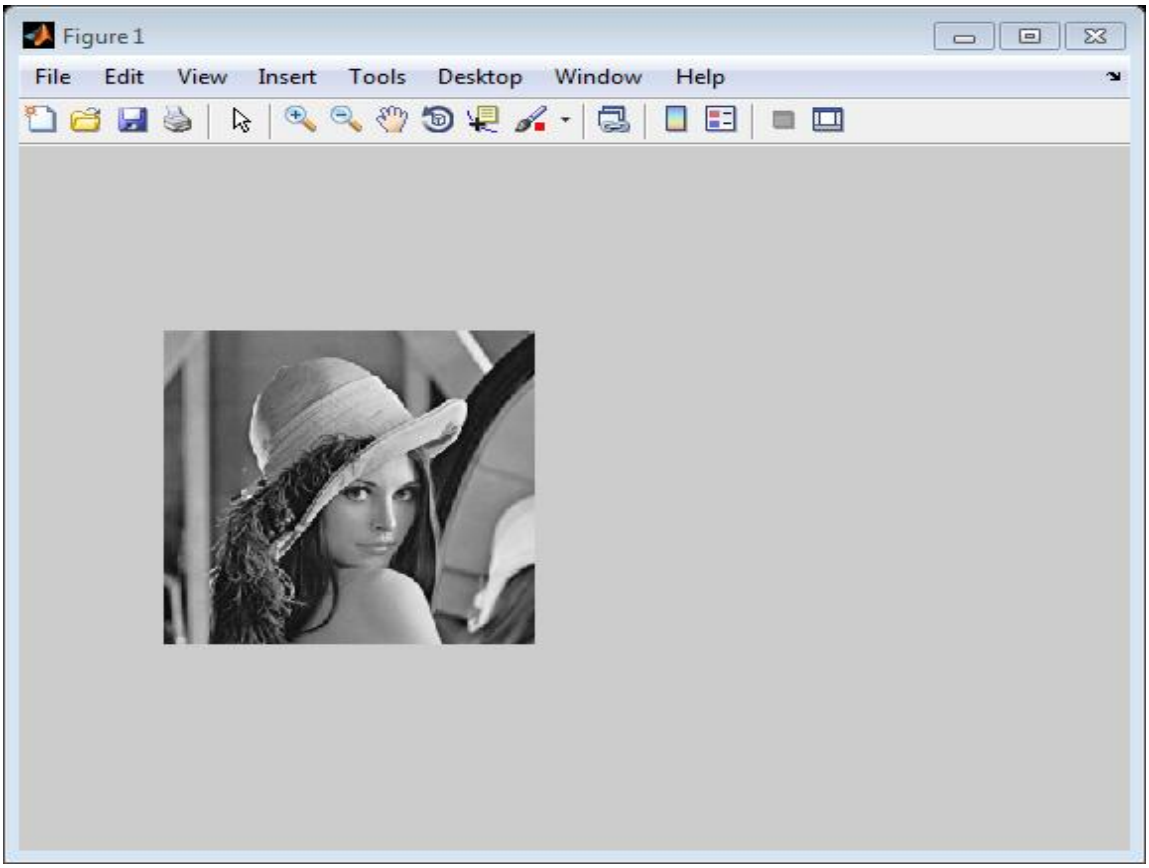

Figure 14: Extraction of the original image

References

F.A.P Petitcolas, R.J. Anderson and M.G.Kuhn; "Information Hiding a Survey",Proceedings of the IEEE, vol.-87, issue 7, pp. 1062-1078, 1999.

S. Dumitrescu, W. X. Wu and N. Memon, "On steganalysis of random LSB embedding in continuous-tone images", Proc. International conference on image Processing, Rochester, NY, pp.641-644, 2002

Beenish. Mehboob and Rashid Aziz Faruqui,"A steganography Implementation", IEEE-Symposium on Biometrics & Security technologies, ISBAST' 08, 23-24, April, 2008 Islamabad.

K. Ahsan, & D. Kundur, "Practical data hiding in TCP/IP", Proceeding of the workshop on multimedia security at ACM multimedia, 2002.

A.Westfeld, "F5-A steganographic algorithm: High capacity Despite Better Steganalysis", Proc.4th Int'l Information Hiding. Workshop, Springer,Verlag vol. 2137, New York, 2001.

I. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia". IEEE Transaction on Image processing,Vol 6, issue 12, pp1673-1687, 1997.

Jiri Fridrich ." A New Steganographyic Method for Palette-Based Images". Center for Intelligent Systems, SUNYBinghamton, Binghamton, NY 13902-6000. U.S Government, a grant number F30602-98-c-0009.

M.Kutter, E. Jordan, and E. Bossen ; "Digital signature of Color images using amplitude modulation", J. Electron Imaging, vol. 7, (2), pp.326-332, 1998.

E.T. Lin, E.J. Delp. "A review of data hiding in images", Proceedings of the conference on image process image quality image capture systems, PICS'99'. 25-28, April 1999, savannah, Georgia, pp. 274-278

BENDER, W. GRUHL, D. MORIMOTO N, and A. LU, "Techniques for data Hiding", IBM, syst. J., 35, (3&4) pp.313-336, 1996.

S. K. Moon and R.S. Kawitkar, "Data Security using Data Hiding", IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

KO-Chin Chang, Chien-Ping Chang, Ping S.Huang, and Te-mingTu.:"A novel image steganographic method using Tri-way pixel value Differencing".Journal of multimedia, Vol.3, No.2, June-2008.

K.Suresh Babu, K. B. Raja , Kiran Kumar k , Manjula Devi T H, Venugopal K R ,L.M Patnaik. "Authentication of secret information in image steganography;"TENCON-2008, IEEE Region 10 Conference. pp. 1-6, Nov 2008.

Biographical notes:

Mrs. G.Aparna obtained B.E degree in Electronics and Communication Engineering from Osmania University, Telangana, India in 2001 and M.E in Systems and Signal Processing from Osmania University, Telangana, India in 2006. At present, she is pursuing Ph.D from Osmania University, Telangana. She possesses one and half decades of teaching experience blended with 3 years of research exposure. Currently she is associated with Aurora's Group, Hyderabad, in the capacity of Associate Professor in the Department of ECE. Her research interests are Signal Processing, Communication Systems, Network Security. Email-aparnaece27@gmail.com.

Dr. M. KEZIA JOSEPH , Professor, Dept of ECE, Stanley College of Engineering and Technology for Women, Nampally, Hyderabad, India. Dr.M.Kezia Joseph born in 1981 in India, obtained B.Tech (ECE) from JNTUK and M.Tech (B.E) from IIT Madras and PhD from JNTUK in Digital Image Processing. She has teaching experience of 13 years serving Engineering College in ECE Department. At present she is associated with Professor, Department of ECE ,Stanley College of Engineering& Technology for Women& , Nampally, Hyderabad, India. Her areas of interest are Signal, Image and Video Processing and Artificial Intelligence. Email: keziajoseph@stanley.edu.in.

Professor C.N.Sujatha, obtained B.Tech in Electronics and Communication Engineering, V.R Sidharatha Engineering College, Nagarjuna University, Vijayawada, India, 2001. M.Tech in ECE Department, Sri Venkateswara University, Tirupati, India 2005. Ph.D in ECE Department – Digital Image Processing, Sri Venkateswara University, India in 2018. She has 16 years of academia teaching (UG and P.G) in ECE Department. Presently she is Professor in Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India. Her Research Interests are Signal Processing, Image and Video Processing, Machine Learning, Deep Learning and Antenna Design. Email: cnsujatha@sreenidhi.edu.in.