Steg Crypt (Encryption using steganography)

Naveen Chandra Gowda, P. Sai Venkata Srivastav, Guru Prashanth.R, Raunak.A, Madhu Priya R

Abstract-The target of this venture is to obtain secured encryption and authentication using steganography. So as to accomplish this, numerous organizations & universities in the world have given solutions to secured communication, in the interim many algorithms have been created, including like AES, RSA, LSB etc. But though these algorithms have been developed they were endured to breakdown by hackers which make them obsolete. In this paper we try to combine many already existing algorithms like AES, LSB into one proposed system. Firstly, the utilization of steganography along with traditional encryption is implemented in the proposed system. Second, we try to achieve authentication of user using OTP via E-mail. Thirdly, the encrypted data is divided and sent across many servers so it's impossible to get complete encrypted data in one path. By applying the proposed model, the probability of data compromise becomes very minimal and very hard to hack.

Keywords- RSA, AES, LSB, OTP

I. INTRODUCTION

Cybersecurity is that the security of internet associated frameworks, together with instrumentality, programming and knowledge, from cyberattacks. In a very process setting, security includes cybersecurity and physical security each square measure used by endeavours to make sure against unapproved access to server frames and different mechanized frameworks. Knowledge security, that is meant to stay up the privacy, honesty and accessibility of data, could be a set of cybersecurity. As attackers become a lot of ingenious, it's essential to properly outline cyber security and determine what constitutes smart cyber security [1]. Digital security ensures the knowledge associate degreed trustiness of process resources having an area with or interfacing with an association's system. So as to confront attacks like kill chains, zero-day attacks, ransomware, alert fatigue and fund constraints which needs a stronger understanding of those topics and plenty of others. To be able to confront those challenges we want more practical technologies.

The major concern in the security world is data theft, which is considered as a huge problem every corporate companies face. In spite of the fact that individuals have achieved an appearing purpose of desensitization to news referring to an information rupture, securing client information has turned out to be progressively significant in the midst of stricter guideline implementation[1].

Revised Manuscript Received on April 25, 2019.
Naveen Chandra Gowda. Asst. Professor, School of C&IT, REVA University, Bengaluru, India.
P Sai Venkat,School of C&IT, REVA University, Bengaluru, India.
Madhupriya R School of C&IT, REVA University, Bengaluru, India.
Guru Prashanth School of C&IT, REVA University, Bengaluru, India.
Raunak Acharjee School of C&IT, REVA University, Bengaluru, India.

Organizations are never again simply required to declare that their frameworks have been broken yet in addition pay fines.

A data rupture happens once a cybercriminal effectively penetrates associate degree data supply and retrieves delicate information. This could be attainable physically by reaching to a computer or system to require near records or calibration in to the system traffic amid correspondence on the online and taking delicate data like certifications. The last is often the technique wont to target organizations.Thus giving best security amid correspondence or amid information exchange is exceptionally basic. Today world is using encryption to morph the data. According to Techopedia encryption is defined as: Encryption is that the method of victimisation associate formula to rework info type {|to create} it unclear for unauthorized users this scientific discipline methodology protects sensitive knowledge this method of changing from one form to different is termed as encoding.

This paper is organized as section 2 will give the insights on the related work done in the era of applying steganography for hiding the text data in images. Section 3 presents the utilization different techniques used in the proposed system. Section 4 will insights on the actual flow of the proposed methodology. Section 5 throw the light on the results produced and the actual discussion on the results.

II. RELATED WORK

Video watermark algorithms are generally based on relationships between frames and different types of embedding. LSB steganographic method is a very simple but effective method with low computational complexity to embed secret message. Ramalingam et al. [8]used modified LSB algorithm for better efficiency.Bin et al. [9] proposed a data encapsulation method based on motion vectors by using matrix encoding in video. Cao et al [10] proposed a video watermark algorithm based on motion vector as carrier for data hiding method and H.264 video compression process. The principle of "linear block codes" is used here to reduce transformation rates of motion vectors.Kelash et al [11] proposed an algorithm to directly embed data into video frames using color histogram, where pixels of each video frame will be partitioned into two halves, right half will contain hidden bits and left half will contain the counts of right half. Feng B et al. [12] proposed" the syndrome trellis code (STC) with flipping distortion measurement" which compromises capacity but solves the security issue. Tashk A et al. [13] proposed "modified duel watermark scheme" which is in transform domain and gives excellent recovery capacity.

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

Case 1: implementation and analysis of three steganographic approaches [2].

Because of expanding the advancements security frameworks are extremely prevalent in numerous regions. The security of data can be accomplished by utilizing encryption and steganography. In cryptography, scrambled information is transmitted in the wake of changing the other structure rather than the first information. Differentiation cryptography, data concealing procedure can be stretched out for shielding from the fascinating of any assailant. This paper proposes the upgrade security framework by joining these two systems. In this framework, the encoded message is implanted in a BMP picture record. In proposed framework, three LSB steganographic methods have been actualized and dissected. This proposed system intends for data confidentiality, data authentication and data integrity. This framework improves the security of information as well as turns out to be all the more dominant instrument. This framework plans to help compelling ways for securing information. The essential objective of our framework is to improve the security of information and after that to look at three steganographic procedures. At that point we will utilize the upgraded strategy for inserting. In this paper, we simply present three steganographic approaches. In this framework, information is scrambled with RC4 encryption calculation and after that implanted the encoded content in the BMP picture document utilizing three steganographic strategies.

Case 2: A Study and literature Review on Image Steganography [3].

In the present age, the investigation of computerized mixed media content has prompted it being used as a model of sheltered and secure correspondence. The art of secret communication by a secret medium like images is known as steganography as the rival method of detecting the presence of embedded data in media is called steganalysis. In this audit article, we have contemplated and broke down the diverse procedures from different analysts in their exploration. The fundamental objective of picture steganography is to conceal the presence of the information message from the unlawful goal. Picture steganography proposes an occupation to exchange the installed secure information to the objective goal without being distinguished through the unapproved client. Different transporter document arrangements would be utilized, yet advanced pictures are sufficiently vast utilized because of the recurrence and tremendous clients on the overall Internet. To conceal the mystery information in pictures, there are huge scopes of steganographic philosophies exist some are mind-boggling in utilized than others technique. Each strategy has separate solid and frail focuses.

Steganography is one of the significant and exquisite methods used to safely move a mystery message in an indistinct way. Visual Steganography is another additional component of it. It is the steganographic strategy including mixed media documents like pictures, video and so forth to shroud a mystery message. Be that as it may, this strategy may result in the mutilation of the shading frequencies of the spread picture which is unsurprising by some examination. Here in this paper, we have proposed a strategy for steganography which results in
definitely no mutilation of the spread picture. The proposed picture is free of the measure of the spread picture and the mystery picture, for example, a bigger picture can be covered up in a little picture. The proposed strategy additionally utilizes AES Encryption for the secure exchange of the stego-key. The nexus of this spread picture and the encoded information fills the need of secure exchange of mystery information.

Case 3: Analysis of Different Steganographic Algorithms for Secured data Hiding [4].

The importance of steganography is to hide the existence of the information in the protection medium. Steganography and cryptography are partners in computerized security. The undeniable favourable position of steganography over cryptography is that messages don't draw in consideration regarding themselves, to envoys, or to beneficiaries. Additionally, the most recent decade has seen an exponential development in the utilization of media information over the Internet. These incorporate Digital Images, Audio and Video records. This ascent of advanced substance on the web has further quickened the exploration exertion dedicated to steganography. The underlying purpose of this examination was to analysis steganography and the wayit'sexistent. Visible of this work, varied basic techniques for steganography might then be dead and assessed. The qualities and shortcomings of the picked methods would then be able to be stone-broke down. to provide a typical casing of reference the bulk of the steganography techniques existent and examined utilised GIF footage. to create a steganography correspondence abundantmore and more secure the message are often compacted and encoded before being lined up within the transporter. Cryptography and steganography are oftenutilisedalong. Whenever compacted the message can occupy way less areawithin the transporter and can limit the information to be sent. The arbitrary looking message which would result from encryption and pressure would likewise be simpler to cover up than a message with a high level of consistency. In this manner, encryption and pressure are prescribed related to steganography alludes to the investigation of "imperceptible" correspondence. In contrast to cryptography, where the objective is to verify interchanges from a busybody, steganographic strategies endeavour to conceal the very nearness of the message itself from a spectator.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

III. RESOURSE UTILIZATION.

Steganography is concealing personal or mystery infowithin a transporter in Associate in Nursing undetectable approach. It gets from the Greek word steganos, which implies secured or mystery, and graphy (composing or drawing). The medium wherever the mystery infois roofed up is termeda selection medium, this will be photos, video or a sound document. Any steganography calculation evacuates the repetitive bits within theunfold media and supplements the mystery info into house. Higher the character of video or sound more and more repetitive bits area unit accessible for activity [5].
This paper is mainly developed in four phases. First the entered text is encrypted using AES algorithm and then the encrypted text is sent to next phase of encryption. So initially we use traditional encryption algorithm.In the next phase we use TIP (text in picture) encryption using the LSB (least significant bit) algorithm. The encrypted text obtained from previous phase is given as input to this phase where the text is encrypted onto the image. Here we use steganography.

In the third phase we use PIP (picture in picture) encryption using the LSB (least significant bit) algorithm. The picture which was obtained containing the encrypted text is given as input in this stage. In this stage we embed this picture onto a new picture of same size using LSB [6]. In the last stage we divide the picture into many segments and send them via TCP/UDP to different servers. At the other end same steps are followed respectively in order to get back the original text. In order to achieve authentication of the user or message we use OTP via E-mail method, where the receiver must enter his registered mail and an OTP will be sent to the mail. Once the OTP matches the data will decrypt automatically.

The main methodology used in this paper is Steganography. There are many steg algorithms developed these days like
1. Blind side
2. Hide & seek
3. Filter first
4. Battle steg

We use the most time efficient and simplest algorithm called Least Significant Bit (LSB)hiding [7].
This technique is most likely the simplest method for covering up data in a picture but it is shockingly compelling. It works by utilizing the LSB bits of every pixel in one picture to shroud the most critical bits of another. In this way, in a JPEG picture for instance, the accompanying advances the following stepswould need to be taken:

1. Load the initial image to be hidden and target image in which you hide the source image.

2. Next picked the quantity of bits you want to shroud the mystery image in. The lot of bits used within the host image, the lot of it falls apart. Increasing the quantity of bits used but clearly has associate advantageous responseon the mystery image increasing its clearness.

3. Presently you wish to form another image by consolidating the pixels from the 2 footage. On the off probability that you simply select for example, to utilize four bits to shroud the mystery image, there'll be four bits left for the host image. (PGM - one computer memory unit for each component, JPEG - one computer memory unit every for red, green, blue and one computer memory unit for alpha direct in some image types).

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

4. To recover the first picture you simply need to realize what number of bits were utilized to store the mystery picture. At that point filter through the host picture, select the least critical bits agreeing the number utilized ones and after that, utilize them to make another picture with one change. The bit extricated now become the most critical bit.

Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

Hiding depends on the settings you select - however as AN example if we tend to hide within the two least vital bits then, we will hide:

MaxBytes = (image. Height () * image. Width () * 3* 2) /8

i.e. the quantity of pixels, times the quantity of colors (3), times the quantity of bits to cover in, all divided by eight to induce the quantity of bytes. It helps to cover a touch but this as a result of the algorithms could take a moment to search out places that haven't had something hidden in it once us area unit on the brink of the brink.

In this paper we use already existing algorithms like LSB, AES and try to integrate them in one system

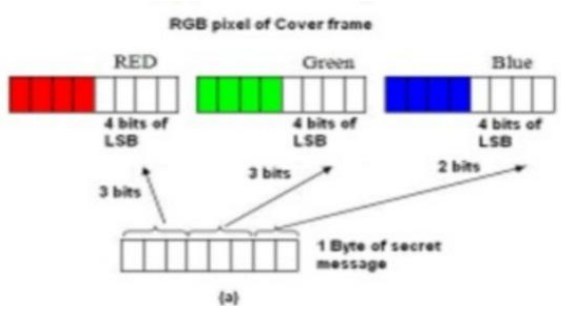

Fig 1: Cover frame

Another algorithm we use is Advanced Encryption Standard (AES) and its steps are as follow [8]:

1. Key extension spherical keys square measure gotten from the figure key utilizing Rijndael's key schedule. AES needs a unique 128-piece spherical key sq. for every spherical

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

additionally to at least one additional

2. Initial round key addition:
   AddRoundKeyeach byte of the state is combined with a block of the round key using bitwise XOR.

3. SubBytes – here we do a non-linear substitution step where every byte is replaced with another according to a lookup table and changed.
   ShiftRows – its a transposition step where the last three rows of the state are changed cyclically to a particular number of steps.
   Mix Columns – it's a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
   AddRoundKey – a combination of block round key using bitwise XOR.

4. Final round (making 10, 12 or 14 rounds in total):
   SubBytes
   ShiftRows
   AddRoundKey

This paper is structured to utilizing the traditional algorithms and steganography algorithm to provide data security and use OTP to provide authentication. It is industrial application is, to be attached to mailing services. It can be linked to the official mailing system where the sender types the information to receiver. The system is automated where user will not have to interfere with the process. At the backend the complete process will done and sent to the specified client. Once the receiver enters the correct OTP the data must decrypt in the backend and show the content to user. This system can be used for many other numerous applications.

IV. METHODOLOGY

The Proposed model majorly has 6 modes, listed below.

OTP Generation: The One Time Password will be generated and shared to the clients, which will be used for authentication at entry level.

Key Management: The followed encryption methodology do require the keys. The 128 bit for AES will be generated and shared among sender and receiver. The random bit key upto 64 bits will be generated by sender and shared to receiver too for using in steganography.

Text Encryption: The input plain text will be encrypted using an efficient AES algorithm.

Text in Picture (TIP): The text data can be hidden the image pixels using steganography. The text bits will be placed in the alpha bits of every pixel bits. So that without affecting the RGB bits of a pixel. So that resultant picture will not have any difference in appearance.

Picture in Picture (PIP): One picture can be hidden in the other picture. Considering the RGB bits of pixels of both image, do apply the steganography. The resultant picture will be having no difference in appearance but has two pictures in it.

Split and forward: The data to be transmitted can be split into segments and transferred individually. Here the image to be transferred will be partitioned into segments, then transfer each segment in different routes. This is to provide the much security against attacks at communication.

The working of the proposed system can be depicted in the Fig 3 and Fig 4. Once the client A got the access to transfer through authentication, the Plain text to be transmitted is taken as input. The plain text will be converted to cipher text using AES encryption with 128 bit key shared by server. The resultant cipher text will be made to hide in a selected random image X using TIP steganography. The resultant of TIP will as same as the random image X in appearance but has hidden text data. The resultant image X then made to hide in another random image Y using PIP steganography. In turn the resultant image will as Y in appearance having image X in it. The PIP resultant image Y will be partitioned into 3 segments of random size using split algorithm. The split data will be routed in different paths to receiver, if available. Expecting all the segments will arrive at the destination without loss or attack. The received segments will be sorted and processed in the reverse order as sender.

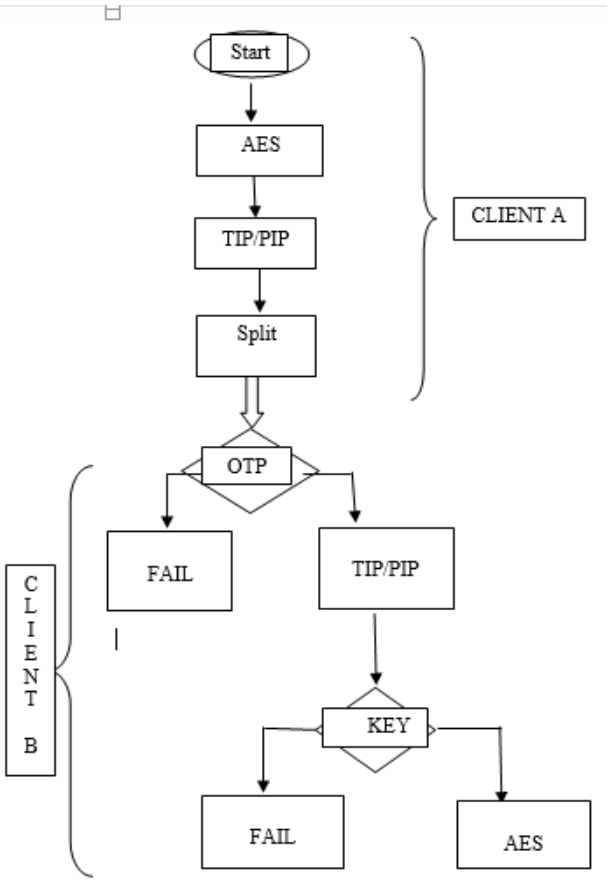

Fig 2: Flow chart of Stegcrypt

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

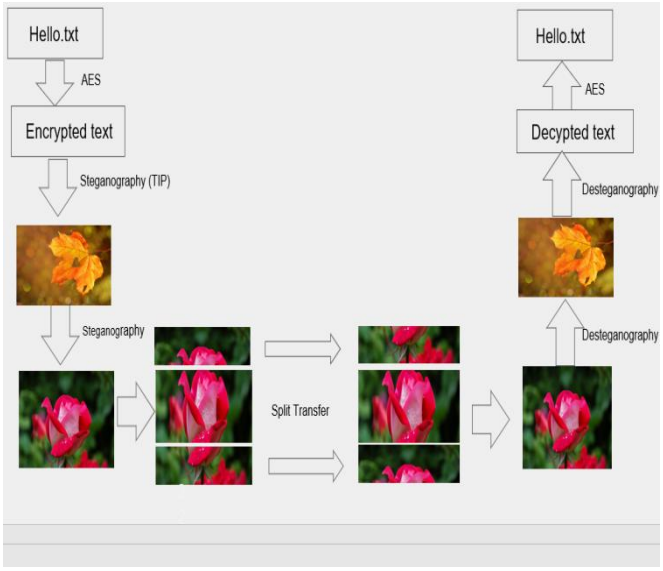

Fig 3: Block diagram of Stegcrypt

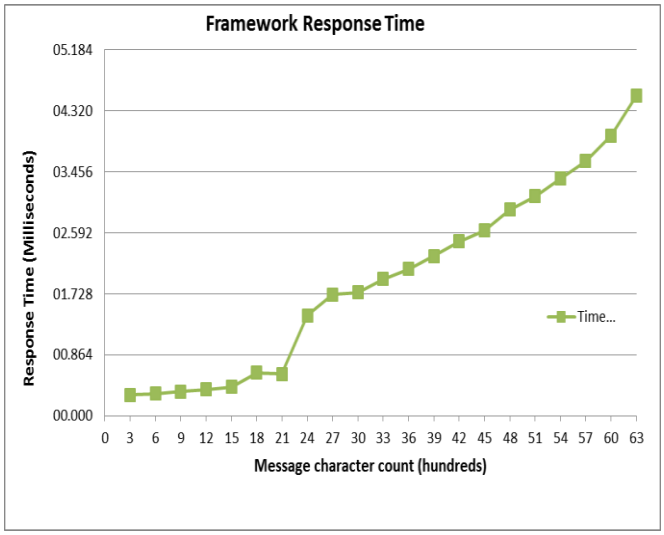

Fig 5: Evaluation ofMessage Character Count with Time

V. RESULTS AND DISCUSSION

The model is designed and implemented in a system with 8GB of RAM and 2GB GPU.

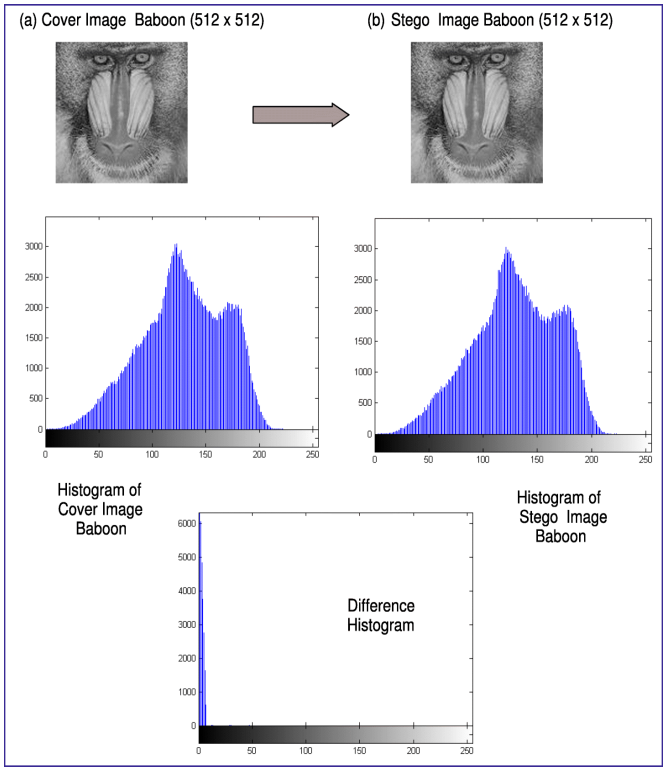

Fig 4: Evaluation of Picture Density

The fig 4 describes, we can find that the picture density for the steganographic image is more compared to original image but the difference is very negligible hence it can be qualified to use an encryption standard.

In the above graph we plot, the response time taken to convert the characters vs the number of characters. The least time taken for three characters is around 00.397 milli seconds. For characters of 63 it takes around 4.700 milli seconds. Our test case for this paper was maximum of 70 characters. This proves that though we combine many algorithms together the time is not that big a constraint for us.

VI. CONCLUSION AND FUTURE SCOPE

The proposed system will be sufficient to combat the security issues faced now days in communication. The effectiveness of the system can be enhanced with help of new algorithms which are more secured.
This system can be integrated with other applications as well. Any area where communication is taking place we can deploy stegcrypt to that system. Compared to other systems its more secure and time efficiency is also very negligible. It can be used in many industrial applications for example

1. We can use it in bank transactions.
2. It can be used for E-mail service
3. It can be used for secure credential sharing.
4. It can be used in hiding data in video

.

In the end every security system becomes obsolete and cannot be failsafe so its required to keep upgrading our security through new policies, new schemes. Our system aims to combine all the existing algorithms together and provide more secure system.

For future scope we want to integrate the existing system with even bank transaction and use more effective

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

Retrieval Number: E10460585S19/19©BEIESP

algorithms and reduce the time component aspect.

VII. REFERENCES

1. Dr. M. Umamaheswari, Prof.S. Sivasubramanian, S.Pandiarajan. Analysis of Different Steganographic Alogorithms for secured data hiding.
2. Achmad Kodar University of Mercu, Implementation of steganography in Image media using LSB.
3. Max Wiess, IJSCRS Vol10, Principles of steganography.
4. E. Cole and R.D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc., ISBN 0-471-44449-9, 2003.
5. IJSPTM Vol 1, No2, Koushik Dasgupta, Hash based least significant big algorithm (HLSB).
6. Feng Pan, Li Xiang, Xiao-Yuan Yang and Yao Guo, Video Steganography using Motion Vector and Linear Block Codes, in IEEE 978-1-4244-6055-7/10/, pp. 592-595,2010.
7. Masud K. S.M. Rahman, Hossain, M.L., A new approach for LSB based image steganography using secret key, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.
8. M. Ramalingam, "Stego machine-video steganography using modified lsb algorithm", World Acad. Sci. Eng. Technol. 74 , 502–505, 2011
9. Z. Li-Yi, Z. Wei-Dong, et al., "A novel steganography algorithm based on motion vector and matrix encoding", in: proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN), IEEE, 2011, pp. 406–409, 2011.
10. Y. Cao, H. Zhang, X. Zhao, H. Yu, "Video steganography based on optimized motion estimation perturbation", in: Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, ACM, pp. 25–31, 2015.
11. H.M. Kelash, O.F.A. Wahab, O.A. Elshakankiry, H.S. El-sayed, "Hiding data in video sequences using steganography algorithms," in: proceedings of International Conference on ICT Convergence (ICTC), IEEE, pp. 353–358, 2013.
12. Deshmukh PU, Pattewar TM, "A novel approach for edge adaptive steganography on LSB insertion technique." In: proceedings of the International conference on information communication and embedded systems (ICICES) IEEE, Chennai, pp 27–28, 2014.
13. Feng B, Lu W, SunW "Secure binary image steganography based on minimizing the distortion on the texture." IEEE Transaction Information Forensics Security 10(2):243–255, 2015

AUTHORS PROFILE:

P. Sai Venkata Srivastav is currently pursuing B.TECH in Computer Science and Engineering at REVA University Bengaluru, Karnataka, India
EMail: slbsaiga@gmail.com

Madhu PriyaR. is currently pursuing B.TECH in Computer Science and Engineering at REVA University Bengaluru, Karnataka, India
EMail: rmadhupriya16@gmail.com

P. Guru Prashanth Rao is currently pursuing B.TECH in Computer Science and Engineering at REVA University Bengaluru, Karnataka, India
EMail: guruprashanth.rao@gmail.com

Raunka.A is currently pursuing B.TECH in Computer Science and Engineering at REVA University Bengaluru, Karnataka, India
EMail: raunakacharjee@gmail.com

Naveen Chandra Gowda is an Assistant professor of School of C&IT in REVA University, Bengaluru, Karnataka, India
EMail: naveenchandrag@reva.edu.in

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication