“Image Steganography Using Kmeans & Encryption”

line 1: 1st **Arju Lokhande**
line 2:*dept.*
(Department of Computer science and Engineering)
line 3: *name of organization*
(Jhulelal Institute of Technology)

line 4: City, Country
Nagpur, Maharashtra, India

line 1: 2nd **Diksha Shelke**
line 2:*dept.*
(Department of Computer science and Engineering)
line 3: *name of organization*
(Jhulelal Institute of Technology)

line 4: City, Country
Nagpur, Maharashtra, India

line 1: 3rd **Prachi Pagare**
line 2:*dept.*
(Department of Computer science and Engineering)
line 3: *name of organization*
(Jhulelal Institute of Technology)

line 4: City, Country
Nagpur, Maharashtra, India

line 1: 4th **Pooja Jawade**
line 2:*dept.*
(Department of Computer science and Engineering)
line 3: *name of organization*
(Jhulelal Institute of Technology)

line 4: City, Country
Nagpur, Maharashtra, India

line 1: 5th **Mrs. Kalpana Bhure**
line 2:*dept.*
(Department of Computer science and Engineering)
line 3: *name of organization*
(Jhulelal Institute of Technology)

line 4: City, Country
Nagpur, Maharashtra, India

Abstract : Nowadays, the community has important roles for transferring records precisely and quick from source to a destination. In this project we are develop new algorithm to Image Steganography Using Kmeans & Encryption technique Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. In this paper, we review the different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, MLSB etc. Most of the existing steganographic algorithms are performed in pixel domain as it provides more embedding space (capacity), reliability and controllability in encoding/decoding of the hidden message.

Keywords : ***Steganography, Stego- image, LSB, ISB, MSB***

*Introduction (*Heading 1*)*

- Steganography, which is Greek for "covered writing," is a subset of the emerging discipline of information hiding. It is the science of transmitting a message between two parties in such a manner that an eavesdropper will not be aware that the message exists. Unlike cryptography, which seeks to hide the content of the message, with steganography we seek to hide the existence of the message. Of course, steganography and cryptography can be used in conjunction, so that message content may be protected cryptographically, even if the steganographic "shield" fails and the existence of the message is discovered.
- Today digital data can be easily copied and multiplied without information loss. It has become imperative to verify the owner of a digital data, to identify illegal copies of the multimedia content and to prevent unauthorized distribution. Information hiding techniques have thus recently received great attention from the research community.
- Steganography involves hiding of text, image or any sensitive information inside another image, video or audio in such a way that an attacker will not be able to detect its presence.
- Steganography is, many times, confused with cryptography as both the techniques are used to secure information.
- The difference lies in the fact that steganography hides the data so that nothing appears out of ordinary while cryptography encrypts the text, making it difficult for an outsider to infer anything from it even if they do attain the encrypted text.
- Both of them are combined to increase the security against various malicious attacks. Image Steganography uses an image as the cover media to hide the secret message.

- In this project, we propose an image steganography method which clusters the image into various segments and hides data in each of the segment. Various clustering algorithms can be used for image segmentation. Segmentation involves huge set of data in the form of pixels, where each pixel further has three components namely red, green and blue. K-means clustering technique is used to get accurate results. Therefore, we use K-means clustering technique to get accurate results in a small time period.

• Literature Survey

[1] Hiding information in images, L.M. Marvel, C.T. Retter, C.G. Boncelet (2011) We have presented a novel steganographic methodology that uses error control coding, image processing, and spread spectrum techniques. This process provides a method for concealing a digitalsignal within a cover image without increasing the size of the image. Additionally, cover image escrow is not needed due the image restoration resulting in a more practical system. A level of security is provided by the necessity that both sender and receiver possess the same public or privatekeys. Furthermore, the embedded signal power is insignificant compared to that of the cover image.This insignificance provides low probability of detection, and thereby leaves an observer unaware that the hidden data exists.

[2] New Data Hiding Algorithm inMATLAB Using Encrypted Secret Message, Agniswar Dutta, Abhirup KumarSen, Sankar Das, Shalabh Agarwal (2011) In the present work we try to embed some secret message inside any cover file in encrypted form so that no one will be able to extract actual secret message. The program developed in MATLAB. We embed LSB and LSB+3 bits of the cover file in every alternate byte position. The encryption of the secret message file here we have taken 5 times but one can go up to any limit. But if we increase the encryption number then the process becomes slow but the encryption will be very strong. In principleit will be difficult for anyone to decrypt the encrypted message without knowing the exact encryptionmethod. Our method is essentially stream cipher method and it may take huge amount of time if the files size is large and the encryption number is also large. This present method may most suitable for water marking. The steganography method may be further secured if we compress the secret messagefirst and then encrypt it and then finally embed inside the cover file.

[3] Implementation and Comparison of different Data Hiding Techniques inImage Steganographyy Asha AsokPoornima Mohan(2016) We presented the first wait-free hash table implementation as a proof-of-concept for the design and implementation of our LC/DC library of nonblocking algorithms and data structures. Our hash table implementation provides the progress guarantee of wait-freedom with a performance improvement over thebest available locking solution and all tested lock free solutions. We discussed the relevance of this work andits applicability in the real-world. As modern and future architectures feature many cores, large number of threads, and greater sharing of information, it is essential to explore such novel paradigms for concurrent software design. The envisioned library implementation and the associated programming interface and optimization support will provide an immense productivity and performance boost for developers of existingand future scientific and systems applications, which are predominantly in C/C++.

[4] SteganographyBased Data Hiding forSecurityApplications G. Ramya; P.P. Janarthanan; D. Mohanapriya (2018) In future, the proposed technique can be enhanced so that the processing time can be reduced. Further, in the present system, only the audio signals are used. In future, the audio signals from any instrument can be taken directly. Instead of LSB algorithm, the other algorithms like threshold-basedsteganography may be used for audio and image steganography at different stages. The proposed technique can be used in real time applications such as Ecommerce, banking, and military and so onfor security purposes.

[5] Hiding The Text into AnImage By Max-Plus Algebra Kiswara Agung Santoso; AhmadKamsyakawuni;Abduh Riski (2018) Image Steganography is a technique that finds applications in many fields, for purposes like data hiding or storing confidential data. Many varieties of Image steganography techniques are available nowadays So, the selection a particular technique depends on its efficiency. By comparing the above-mentioned methods, it can be seen that LSB Substitution with some amount of encryption is the betterone among them. PVD substitution on the other hand provides better imperceptibility but is more complex than LSB substitution based on similarity of bit pairs.

[6] A Novel Approach toHide Text Data in Color Image, Suraj Kumar; Santosh Kumar; NeerajKumar Singh; Anandaprova Majumder The proposed method in the paper, selectively feeds the pixels with secret data. The noise bed hence obtainedis not so distorted as to arouse suspicion. The histogram of the stego image shows subtle variation from original cover image, hence affirming better visual quality in comparison to generic LSB approach. The PSNR ratio shows greater value than the generic LSB substitution method which signifies the low distortion of the image due to embedding of the secret data in it. This factor of embedded distortion would behaviorally be in alignment to the natural distortion gained by the image in the transmission channel. Hence the anomaly in the image, howsoever small, detected by the steganalysis algorithm is more likely to be overlooked on the account of the transmission channel noise.

[17] In this paper data security has been proposed By using RSA encryption technique and by calculating hash value with distributed verification of erasure coded data, correctness as well as preserving privacy of data in cloud.

[18] Here Segmented images are used for hiding the data using DES algorithm has been done by the authors

[19] Here authors have collected a details survey on cloud load balancing with few securities mechanism

[20] In this paper authors proposed the security mechanism to data using hash and some encryption technology

• Proposed System

The original aims of the paper are to introduce a technique for hiding a text file, which techniques hide a secret text file inside an image file, and the modified image must be similar to the original image, in other words the changes that happen on the modified image mustn't be visible, or the human eye would be unable to notice it.

The project application loads 24-bit BMP, GIF, and JPG image format, embed data into them using Sunflower system and saves the images. Encryption can be used before embedding the data to provide robustness. Finally, the application can also extract data that was previously embedded. The application runs in a user friend Windows environment where the user can view the image, before and after the embedding. The Proposed Structure of Sunflower System structure of the proposed system is shown below:

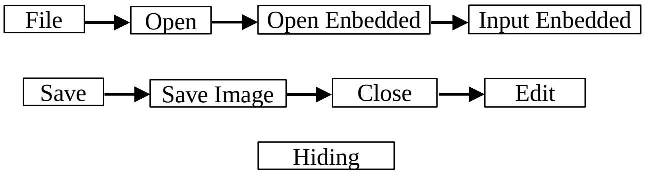

Fig. structure of the proposed system

- ## Conclusion

In this research work we reviewed many papers on steganography techniques. These papers are good enough and have wide future scope. By reviewing these papers, we observed that most of the steganography work is done in the year 2012 & 2013. In these years, LSB is the most widely used technique for steganography. Some researchers have also used the techniques like water marking, distortion technique, spatial technique, ISB, MSB in their work and provided a strong means of secure information transmission. Most of the papers that are discussed here are taken from IEEE Explore, AICCSA, IJET, IJCSE, IJCA etc. This review paper is enough for them to start their work in this field. The different security and data hiding techniques are used to implement steganography using LSB, ISB, MLSB.

- ## Future Scope

Hiding a file, message or even a video within another file can be an effective way for malware authors to obscure their own payload or to exfiltrate user data. Given the popularity of image sharing on social media sites and the prevalence of image-based advertisement, we expect the recent trend of using steganography in malware to continue. These papers provide a lot of help to the initiator for starting their work in this field. In further research we are going to use more advance schemes like steganography with some hybrid cryptographic algorithm for enhancing the data security.

REFERENCES

[1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., “Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography”, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2] Swati malik, Ajit “Securing Data by Using Cryptography with Steganography” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[3] Ishwar jot Singh, J.P Raina, “Advance Scheme for Secret Data Hiding System using Hop field & LSB” International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[4] G. Manikandan, N. Sairam and M. Kamarasan “A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme “, Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012.

[5] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, “Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique”, International Conference on Emerging Trends in Science, Engineering and Technology, pp.192-197, July 2012.

[6] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, “Extracting spread-spectrum hidden data from digital media “, IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[7] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., “A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[8] Bailey, K., and Curran, K., “An Evaluation of Image Based Steganography Methods”, Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[9] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, “Triple-A: Secure RGB Image Steganography Based on Randomization”, International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[10] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , “Colour Guided Colour Image Steganography” Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.

[11] Anil Kumar, Rohini Sharma,”A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique “,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[12] Gutub, A., Al-Qahtani, A., and Tabakh, A., “Triple-A: Secure RGB image steganography based on randomization”, Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403, 2009... [13] Dr. Fadhil Salman Abed “A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography “, IJAIEM, Volume 2, Issue 4, April 2013.

[14] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, “Authentication of secret information in image steganography”, IEEE Region 10 Conference, TENCON- 2008, (2008) November, pp. 1-6

[15] M. Chaumont and W. Puech, “DCT-Based Data Hiding Method to Embed the Color Information in a JPEG Grey Level Image”, 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, (2006) September 4-8.

[16] A. M. Hamid and M. L. M. Kiah, “Novel Approach for High Secure and High-Rate Data Hidden in the Image Using Image

Texture Analysis", International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[17] Chandu Vaidya and Prashant Khobragade. " Data Security in Cloud Computing". International Journal on Research and Innovation Trends in Computing and Communication, 2015. Volume ,3. Issue.5. ISSN: 2321-6169. pp: 167-170.

[18] Sampritha S. Shetty "Image Steganography Using K-Means and DES Algorithm" International Journal of Research in Engineering, Science and Management Volume-3, Issue-6, June-2020 www.ijresm.com | ISSN (Online): 2581-5792

[19] Vaidya, C., and Bhure, K. S. (2020). Survey on Cloud Computing Load Balancing. *i-manager's Journal on Cloud Computing*, 7(1), 32-46. https://doi.org/10.26634/jcc.7.1.17156

[20] Chandu Vaidya, Prashant Khobragade and Ashish Golghate, "Data Leakage Detection and Security in Cloud Computing", GRD JournalsGlobal Research Development Journal for Engineering,Volume 1,Issue 12,November 2016.

[1] ***Authored book:*** Woods, D. D. and E. Hollnagel. 2012. *Joint cognitive systems*. Boca Raton: CRC Press/Taylor & Francis.

In text: (Woods and Hollnagel 2012)

[2] ***Chapter in multi authored book:*** Wiens, J. A. 2005. Avian community ecology: An iconoclastic view. In *Perspectives in ornithology*, ed. A. H. Brush, and G. A. Clark, 355–403. Cambridge: Cambridge Univ. Press.

Note: In Reference section, when there are more than six authors, first three are listed, followed by et al. In text, first author listed followed by et al.

[3] **Journals:** Terborgh, J. 2009. Preservation of natural diversity. *BioScience* 24:715-22.

Electronic journal: Testa, B., and L. B. Kier. 2013. Emergence and dissolvence in the self-organisation of complex systems. *Entropy* 2, no. 1 (March): 1-25. http://www.mdpi.org/entropy/papers/e2010001.pdf.

[4] **Unpublished Documents***:*Schwartz, G. J. 2012. Multiwavelength analyses of classical carbon-oxygen novae. PhD diss., Arizona State Univ.

O'Guinn, T. C. 2014. Touching greatness. Paper presented at the annual meeting of the American Psychological Association, New York.

[5] **Online Documents**: Adamic, L. A., and B. A. Huberman. 2006. The nature of markets in the World Wide Web. Working paper, Xerox Palo Alto Research Center. http://www.parc.xerox.com/istl/groups/iea/www/webmarkets.html (accessed March 12, 2014).

U.S. Census Bureau. 2013. Health insurance coverage status and type of coverage by sex, race, and Hispanic origin. Health Insurance Historical Table1. http://www.census.gov/hhes/hlthins/historic/hihisttl.html.

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord “Format” pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

Font- Times New Roman, 09/10 pts

Line spacing-1.2