

PROJECT REPORT
ON
Image Steganography Using K-means & Encryption

Submitted in partial fulfillment of the award of degree of
Bachelor of Engineering
(Computer Science & Engineering)

Submitted by:

Arju Lokhande
Diksha Shelke
Prachi Pagare
Pooja Jawade

B.E., Computer Science & Engineering
JIT, Nagpur

Guided by:

Ms. Kalpana Bhure
Asst. Professor, Computer Science Engineering
JIT, Nagpur



Department of Computer Science & Engineering
Jhulelal Institute of Technology
Session 2021-22



Jhulelal Institute of Technology
Nagpur

Jhulelal Institute of Technology

Department of Computer Science and Engineering

Off Koradi Road, Lonara, Nagpur Tele: +91-712-2668234, +91-712-2668235

Email: cse@jit.org.in Visit us at: <http://www.jitnagpur.edu.in/>

College Vision

To become an eminent institution through knowledge and research.

College Mission

To produce world class engineers with academic and moral excellence who are not only equipped with cutting edge technology skills but also possess immense sense of social responsibility.

To inculcate awareness and acceptance of ethical values through co-curricular activities for overall development of students.

Department Vision

To become as a one of the best technology departments through education, development of technical skills and collaborative research.

Department Mission

The mission of the department is,

- 1) To provide quality education to students.
- 2) To grow technically and give more knowledge for the betterment of mankind.
- 3) To develop e-awareness in students and society in general.

PROJECT REPORT
ON
Image Steganography Using K-means & Encryption

Submitted in partial fulfillment of the award of degree of
Bachelor of Engineering
(Computer Science & Engineering)

Submitted by:

Arju Lokhande

Diksha Shelke

Prachi Pagare

Pooja Jawade

B.E., Computer Science Engineering

JIT, Nagpur

Guided by:

Ms. Kalpana Bhure

Lecturer, Computer Science Engineering

JIT, Nagpur



Department of Computer Science & Engineering
Jhulelal Institute of Technology
Session 2021-22

DECLARATION

I hereby declare that the thesis entitled “**Image Steganography Using K-means & Encryption**” submitted here

in has been carried by us in the Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur. The work is original and has not been submitted earlier as a whole or in part for the award of any degree/ at this or other Institution/University.

Date

Arju Lokhande

Diksha Shelke

Prachi Pagare

Pooja Jawade

Department of Computer Science & Engineering

Jhulelal Institute of Technology

Session 2021-22

CERTIFICATE

This is to certify that the report entitled “**Image Steganography Using K- means & Encryption**” submitted to the Rashtrasant Tukdoji Maharaj Nagpur University, Nagpur in partial fulfillment of the requirement for the award of a degree of Bachelor of Engineering in Computer Science & Engineering. The record of the candidates own work carried out under our supervision at the Department of computer Science and Engineering, Jhulelal Institute of Technology, Nagpur during the academic year 2021-22. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Ms. Kalpana Bhure
Asst Prof, CSE
Project Guide

Mr. Anup Khadakkar
Project Developer , Nagpur
Industry Guide

Ms..Mona Mulchandani
HOD, CSE
JIT, Nagpur

Dr. Narendra Bawane
Principal
JIT, Nagpur

Department of Computer Science & Engineering
Jhulelal Institute of Technology
Session 2021-22

ACKNOWLEDGEMENT

We would like to take this opportunity to acknowledge our profound indebtedness and extend our deep sense of gratitude to our respected guide Mr. **Anup Khadakkar, Intechzia** and also our respected guide **Prof. Kalpana Bhure**, Department of Computer Science & Engg. for their valuable guidance, profound advice and encouragement that has led to the successful completion of this project.

We are grateful to our respected **HOD Prof. Mona Mulchandani**, Department of Computer Science & Engg for her full cooperation and help. We also thank the staff members of the CSE department.

Our sincere thanks to respected **Dr. Narendra Bawane, Principal, JIT**, for providing us the necessary facility to carry out the work.

We would like to thank all the people who have directly and indirectly help us in the completion of our project.

Finally we would like to express our deepest gratitude to our parents for encouraging through the progress in the work.

Abstract

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.

List of Figures

Figure No.	Title	Page No.
5.1	Data flow diagram for Image Steganography Using Kmeans & Encryption	11
7.1	Admin login page.	15
7.2	Admin can see what are the queries of the user.	16
7.3	User login page	16
7.4	User Registration Page	17
7.5	Shows User can send any data and Query.	17

List of Symbols

Abbreviation	Meaning
PSNR	Peak signal-to-noise ratio
BER	Bit Error Rate
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
ISB	Information System For Biotechnology
MSB	Most Significant bit

List of Publication

Sr. No.	Paper Title
1	A Review Paper on Image Steganography Using Kmeans and Encryption
2	Securing Data Using Image Steganography And Encryption Techniques

CONTENTS

<i>Candidate's Declaration</i>	
<i>Acknowledgement</i>	<i>i</i>
<i>Abstract</i>	<i>ii</i>
<i>List of Figures</i>	<i>iii</i>
<i>List of Tables</i>	<i>iv</i>
<i>List of Symbols</i>	<i>v</i>
<i>List of Publications</i>	<i>vi</i>
Chapter 1 – INTRODUCTION	1
Chapter 2 – LITERATURE REVIEW	3
Chapter 3 – AIM & OBJECTIVES	6
3.1 Aim	
3.2 Objectives	
Chapter 4 – PROPOSED METHODOLOGY	8
Chapter 5 – CONCEPTUAL DESIGN DATA FLOW	
DIAGRAM	10
Chapter 6 – SOFTWARE & HARDWARE	12
REQUIREMENTS	
6.1 Software Requirements	
6.2 Hardware Requirements	

Chapter 7 – IMPLEMENTATION	14
Chapter 8 – RESULT ANALYSIS & DISCUSSION	18
Chapter 09 – ADVANTAGES, DISADVANTAGES	21
10.1 Advantages	
10.2 Disadvantages	
CONCLUSION	23
FUTURE SCOPE	24
REFERENCES	25
ANNEXURE	27

CHAPTER 1

INTRODUCTION

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.[1]

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.

CHAPTER 2

LITERATURE REVIEW

[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 digital signal 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 private keys. 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 in MATLAB Using Encrypted Secret Message, Agniswar Dutta, Abhirup Kumar Sen, 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 principle it will be difficult for anyone to decrypt the encrypted message without knowing the exact encryption method. Our method is essentially stream cipher method and it may take huge amount of time if the file 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 message first and then encrypt it and then finally embed inside the cover file.

[3] Implementation and Comparison of different Data Hiding Techniques in Image Steganography, Asha Asok Poornima 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 the best available locking solution and all tested lock free solutions. We discussed the relevance of this work and its 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 existing and future scientific and systems applications, which are predominantly in C/C++.

[4] Steganography Based Data Hiding for Security Applications 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-based steganography 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 on for security purposes.

[5] Hiding The Text into An Image 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 better one 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 to Hide Text Data in Color Image, Suraj Kumar; Santosh Kumar; Neeraj Kumar Singh; Anandaprova Majumder The proposed method in the paper, selectively feeds the pixels with secret data. The noise bed hence obtained is 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.

CHAPTER 3
AIM & OBJECTIVE

Aim:

Steganography is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. The word steganography comes from Greek steganographic, which combines the words meaning "covered or concealed"

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal.

Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents[5].

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.[1]

Objective:

Steganography is an important technique for information hiding in any digital object. Steganography technique is the science that includes communicating secret information in an appropriate digital multimedia cover objects such as audio, video and image files.

The main objective of steganography is to hide the existence of the embedded data. Steganography technique has improved the security of existing data hiding techniques by the outstanding development in computational power.

Objectives of steganography are Undetectability, robustness and capacity of the concealed data, these key factors that separate it from related techniques like cryptography and watermarking. This paper delivers a survey on digital images steganography and covering its fundamental concepts.

The development of image steganographic methods in spatial representation, in JPEG format and also discuss the recent development in the field of image steganography. Specific generally used approaches for increasing steganographic security are summarized and significant research developments are also discussed.[6]

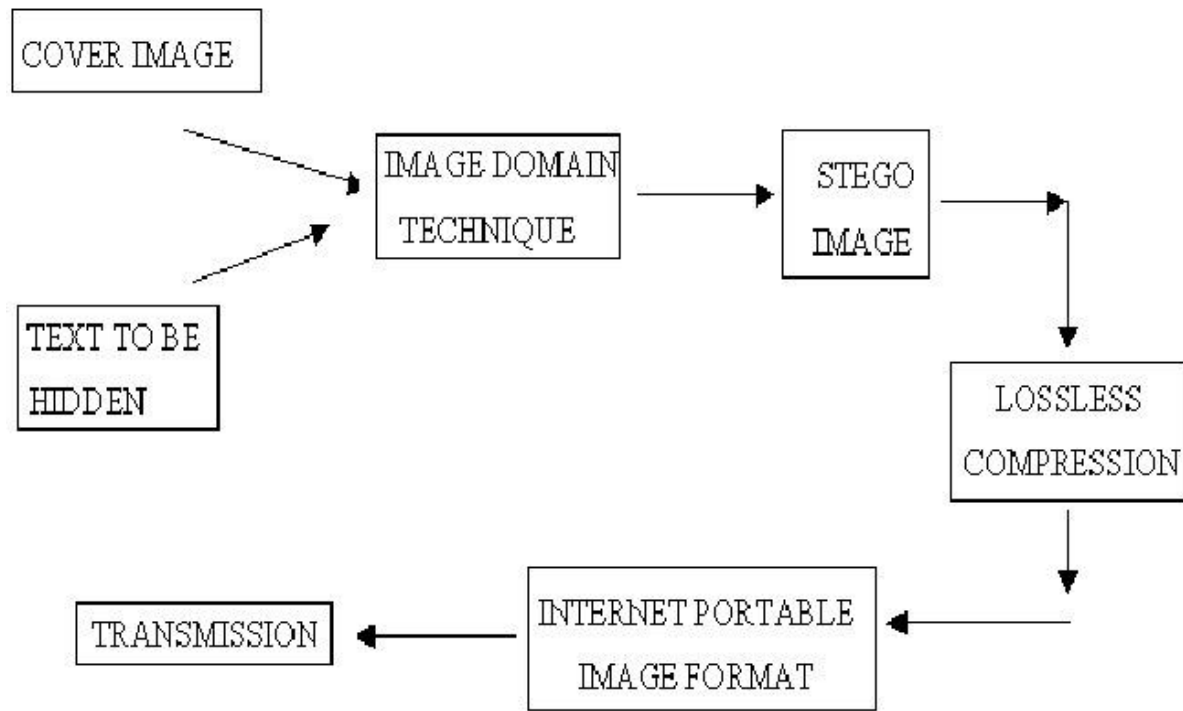
CHAPTER 4

PROPOSED METHODOLOGY

Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. This is a process, which can be used for example by civil rights organisations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to protect the courier. The initial aim of this study was to investigate steganography and how it is implemented. Based on this work a number of common methods of steganography could then be implemented and evaluated. The strengths and weaknesses of the chosen methods can then be analysed. To provide a common frame of reference all of the steganography methods implemented and analysed used GIF images. Seven steganography methods were implemented. The methods were chosen for their different strengths in terms of resistance to different types of steganalysis or their ability to maximise the size of the message they could store. All of the methods used were based on the manipulation of the least significant bits of pixel values or the rearrangement of colours to create least significant bit or parity patterns, which correspond to the message being hidden.[7]

CHAPTER 5

CONCEPTUAL DESIGN DATA FLOW DIAGRAM



Fig(5.1): flow diagram for Image Steganography Using K-means & Encryption

Basic flowchart of Steganographic text embedding. Fig .(5.2) shows flow diagram for Image steganography using K-means and encryption. The techniques for hiding the text behind digital images are broadly classified into two categories: (1) Image Domain Techniques-are entirely dependent upon the image's format (i.e. the way the pixels are arranged inside an image representation). Since pixels are represented by bits, bit manipulation is performed to 'invisibly' modify the color value of certain pixels. As a result, to the human eye the new image looks like the exact replica of the original image. Image domain techniques are generally applied to lossless formats. (2) Transform or Frequency Domain Techniques-are independent on image formats and thus can be applied to lossy formats as well. They involve algorithms and tools that manipulate the image by applying transforms such as DCTs and Wavelet Transformations. They hide messages in more significant areas of the cover image and may manipulate image properties such as their luminance. Hence in these techniques we observe.[6]

CHAPTER 6

SOFTWARE & HARDWARE REQUIREMENT

Software requirement:

- ☐ Google Chrome
- ☐ Sublime Text or Notepad++
- ☐ XAMPP server

Hardware Requirement:

- ☐ i3 Processor with 2.70 GHz Processor
- ☐ 4 GB RAM
- ☐ 160 GB HDD

CHAPTER 7

IMPLEMENTATION

Steganography is classified among the foremost methods employed in data security to conceal and safeguard confidential messages in the data transmitted. Security, especially data security, is an important requisite in today's world hence Steganography has great significance. The paper deals with understanding and implementation of steganography on different images using two different techniques: Least Significant Bit method (secret image is hidden using the bits at least significant level of the cover image) and Discrete Wavelet Transform method (secret image is hidden by modification of the wavelet coefficients of cover image). The image to be transmitted secretly is both encoded and decoded using these methods and a detailed analysis of the resultant images is performed using various image parameters. These experimentally obtained and compared efficiency parameters, thus, demonstrate the efficiency of the methodology proposed in the paper[4]

A) Admin Page

In Admin Page, fig.(7.1)Admin login on this page and see the details of Users. Admin can see How many users have registered, what are the queries of the user etc. fig.(7.2)



Fig: (7.1) Admin login page.

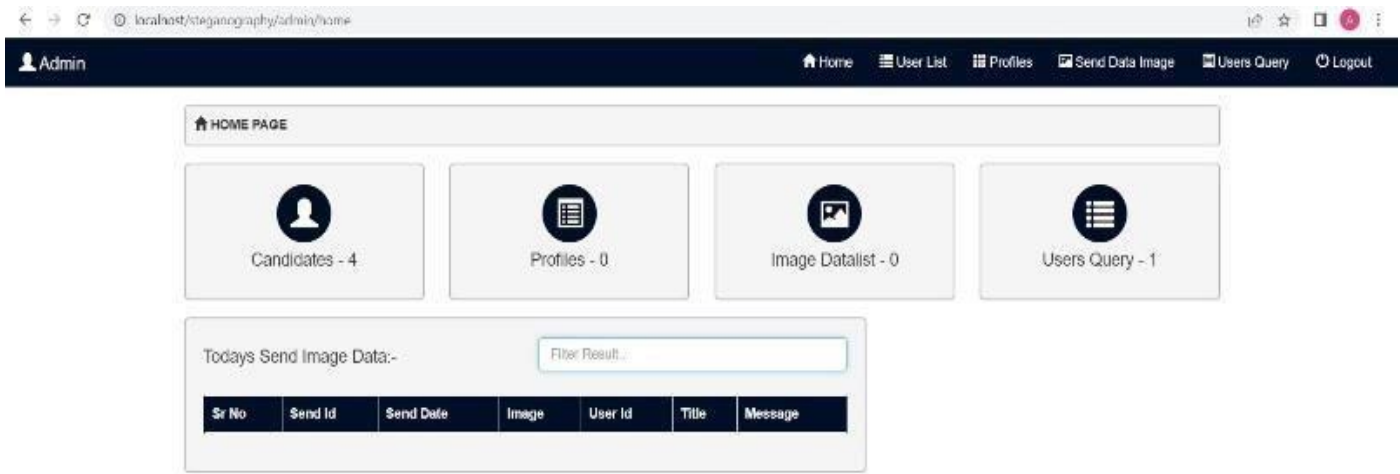


Fig (7.2) Admin can see what are the queries of the user.

B) User Page

In User Page, First User will register on this shown in (7.4)Page then User will login and fill Complete information. User can send any data shown in fig. (7.5)this data will be hidden behind the image. If the user wants to send a query to the admin, the user can Send the query.Fig.(7.3) shows user login page.

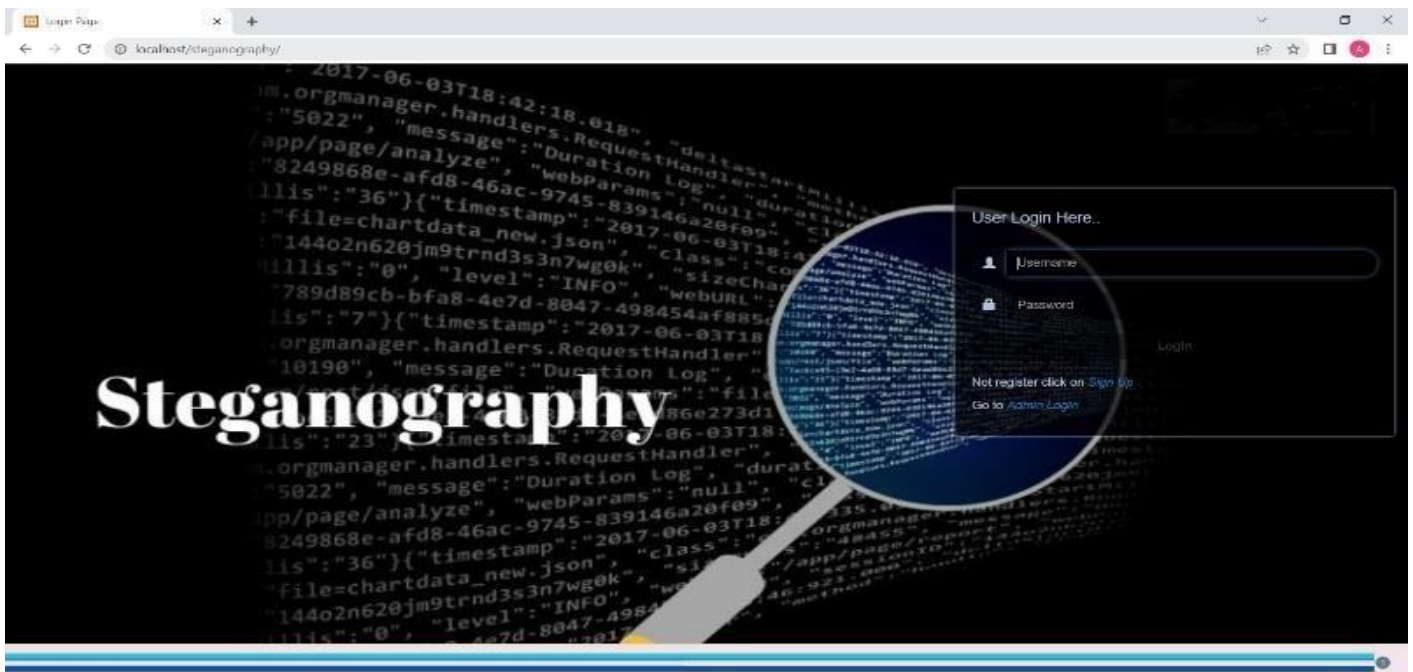


Fig:(7.3) User login Page.

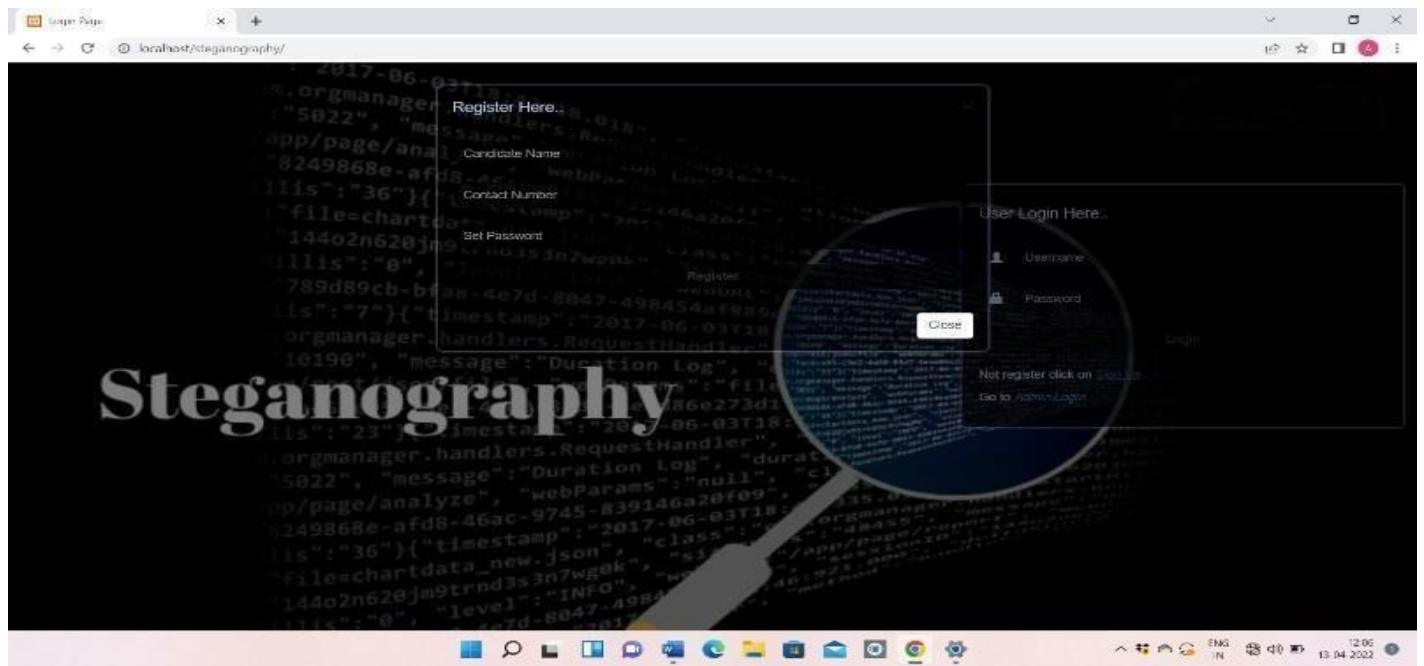


Fig:(7.4) user Registration Page.

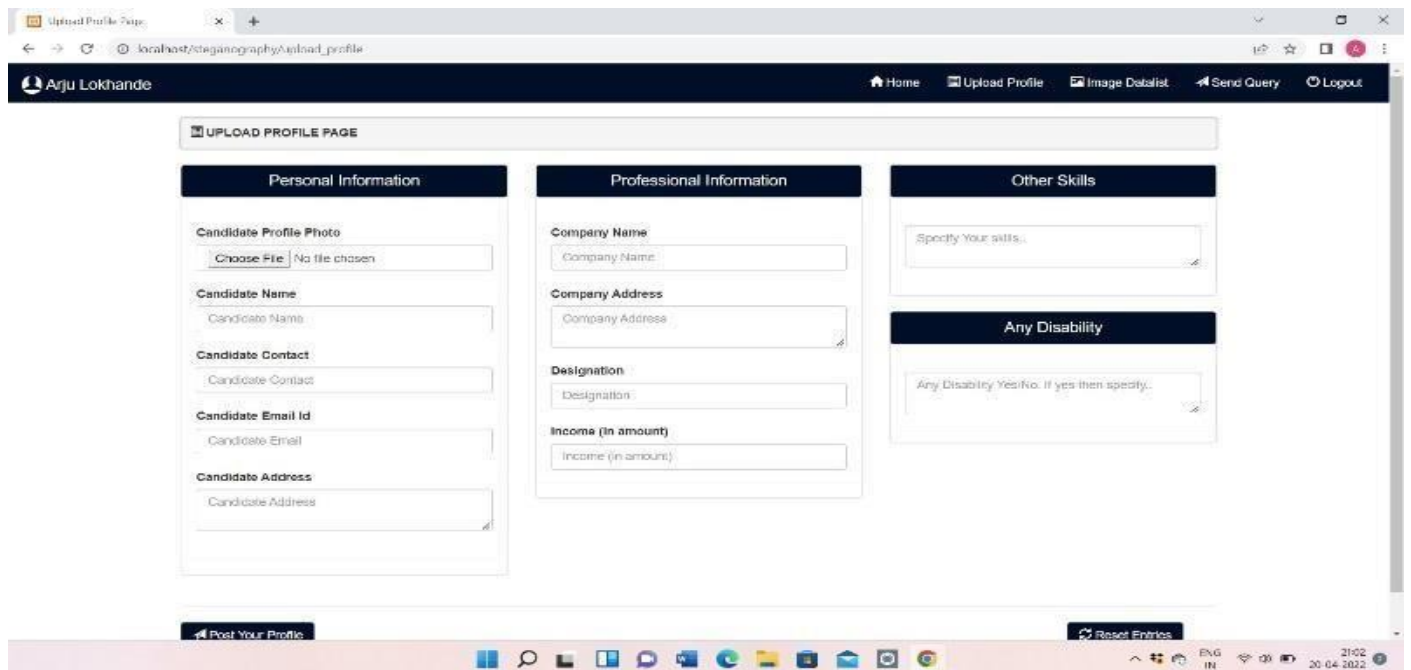


Fig: (7.5) Shows User can send any data and Query.

CHAPTER 8

RESULT ANALYSIS AND DISCUSSION

Analysis

we are introducing the methods to measure the quality and distortion in images. To measure imperceptibility of steganography several metrics are used. To compare stego image and cover results needs a measure of image quality, usually used measures are mean squared error (MSE), peak signal to noise ratio (PSNR) and bit error rate (BER).

1) Mean Squared Error:

Mean Squared Error (MSE) can be calculated by performing byte by byte assessment of the cover file and stego- image. The calculation can be shown as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (f_{ij} - g_{ij})^2$$

From above equation M, N are the number of rows and columns in the Cover image (CVR) matrix, f_{ij} is the pixel value from CVR, and g_{ij} is the pixel value from the stego- image. Higher value of MSE indicates dissimilarity between compared images.

2) Bit Error Rate:

Bit error rate (BER) can be calculated as the actual number of bit positions which are changed in the stego-image compared with CVR.

3) Peak signal-to-noise Ratio:

Peak signal-to-noise ratio measures in decibels the quality of the stego-image compared with the cover file. The higher PSNR the better the quality. The PSNR is computed using the following

$$PSNR = 10 \log_{10} \frac{L^2}{MSE}$$

equation.

PSNR is a good measure for comparing restoration results for the same image

Discussion

We noted that the system was success to satisfy many goals that we can conclude them in the following points:

- First, the recorded PSNR from different experiments shows that the system successes to hide a message in the stego-image without appear notable changes in the stego-image. The system takes the advantage of human visual system which cannot recognize little changes in some pixels of the image. This is the main goal of any steganography system
- Second, the using of the mapping table T in the algorithm of the system is producing to the system the effect of the first of the two main operations in any cryptography system, which is the substitution operation. This is done by the algorithm through mapping a character from the message to more than one value of 7-MSBs of the pixel. Also the mapping table T helps the system to use the second operation of any cryptography system, which is the transposition operation. This can be done by rotating the sequences Seq of characters in the mapping table T to produce many others substitution values for each characters in the message. This can be done at each time that the algorithm takes a next character from the message. Therefore, it is truly that the system works as a cryptography system in addition to its research as a steganography system even if this is done as in simple way

CHAPTER 9

Advantages And Disadvantages /Application

Advantages

- Hard to detect. Original image is very similar to altered image. Embedded data resembles Gaussian noise.
- Hard to detect as message and fundamental image data share same range.
- Altered picture closely resembles original. Not susceptible to attacks such as rotation and translation.
- To hide the existence of a message from a third party.
- Steganography is like detecting microscopic needle in a Haystack.
- We can use this technique in any secret mission. Like Army.

Disadvantages

- Message is hard to recover if image is subject to attack such as translation and rotation.
- Significant damage to picture appearance. Message difficult to recover.
- Relatively easy to detect, as our project has shown.
- Image is distorted. Message easily lost if picture subject to compression such as JPEG.



Jhulelal Institute of Technology

Department of Computer Science & Engineering
Session 2021-2022

“Image Steganography Using Kmeans & Encryption”

Name of Guide: Ms. Kalpana Bhure
Asst. Professor of Computer Science and Engineering
JIT, Nagpur

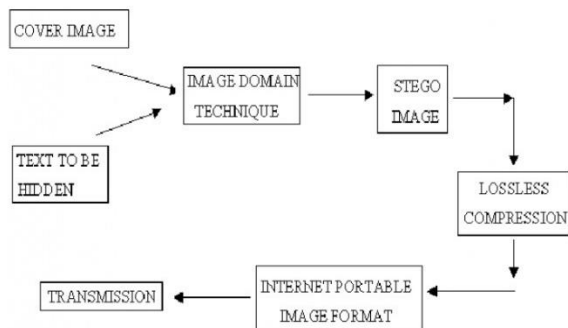
1 Motivation

There are normally two motivations - to send a secret message or to establish authenticity of a piece of information - usually a multimedia file. The later is a major application of modern steganography and known as Digital Watermarking and Fingerprinting.

2 Problem Statement

- The former consists of linguistic or language sort of hidden writing.
- The later, like invisible ink, attempt to hide messages physically. Drawback of this linguistic steganography is that user must equip them to own an honest knowledge of linguistry.
- In recent years everything is trending towards digitalization and with the event of internet technology digital media will be transmitted conveniently over the network. Messages will be secretly carried by digital media using the steganography

3 Flow Diagram



4 Objective

- To test the usefulness of several image steganographic models in banking.
- K means is a clustering algorithm whose main objective and aim is to group similar elements or data points into a cluster.

5 Methodology

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

6 Result

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. The proposed algorithm of the image steganography system is tested by taking different messages of different length and hiding them in some images of different sizes.

7 Project Team

Submitted By:

Ms. Arju Lokhande

Ms. Diksha Shelke

Ms. Pooja Jawade

Ms. Prachi Pagare

Photo With Industrial Guide



Photo With Project Guide



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, (200

ANNEXURE

1) LETTER OF INDUSTRY:



Email : info@intechzia.com

Mob : 9579047478

Website : www.intechzia.com

Date : 09/12/2021

Jhulelal Institute of Technology, Nagpur

This Memorandum of Understanding (MOU) sets for the terms and understanding between **Intechzia** IT Solutions having its office at Alok apartment, canal road, **Dharampeth**, Nagpur and Jhulelal Institute of Technology (JIT), Nagpur, Maharashtra having its office at Lonara, Nagpur to develop **Image Steganography** using **Kmeans & Encryption** Technologies.

These 4 students : -

- 1) Arju Lokhande
- 2) Diksha Shelke
- 3) Pooja Jawade
- 4) Prachi Pagare

And one faculty Ms. Kalpana Bhure (Project Guide) of JIT will be developing this project. Intechzia IT Solutions will provide project training and necessary details required for execution of project as and when required.

We confirm all information is true as per our record.

Regards,



Authorized signatory

Anup Khadakkar

Director

Address : 254, Alok Apartment, Canal road, Dharampeth, Nagpur -10. Contact : 9579047478

2) LETTER OF COMPLETION:



Email : info@intechzia.com

Mob : 9579047478

Website : www.intechzia.com


Date : 22/04/2022

PROJECT COMPLETION CERTIFICATE

This is to certify that **Miss Arju Lokhande , Miss Pooja Jawade, Miss Diksha Shelke and Miss. Prachi Pagare** have successfully completed their project (from 27/11/2021 to 20/04/2022) on **Image Steganography using Kmeans and Encryption** at **Intechzia, Nagpur.**

During the period of their project with us they were found punctual, hardworking and inquisitive. We wish them every success in life.

Regards,



Authorized signatory
Anup Khadakkar
Director

Address : 254, Alok Apartment, Canal road, Dharampeth, Nagpur -10. Contact : 9579047478

1) PROJECT PHOTOS/SCREENSHOTS:



Fig: Admin login page.

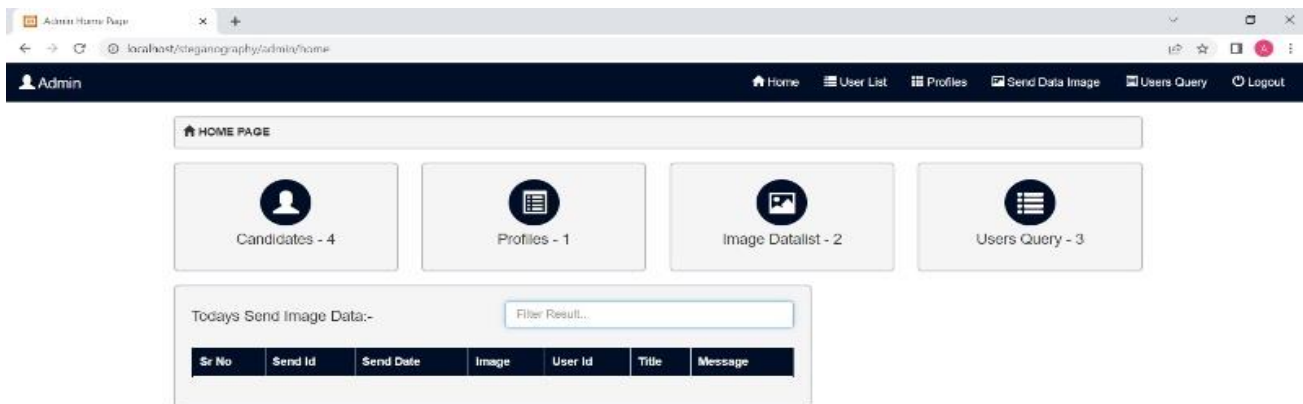


Fig: Shows how many users have registered.



Fig : User login page .

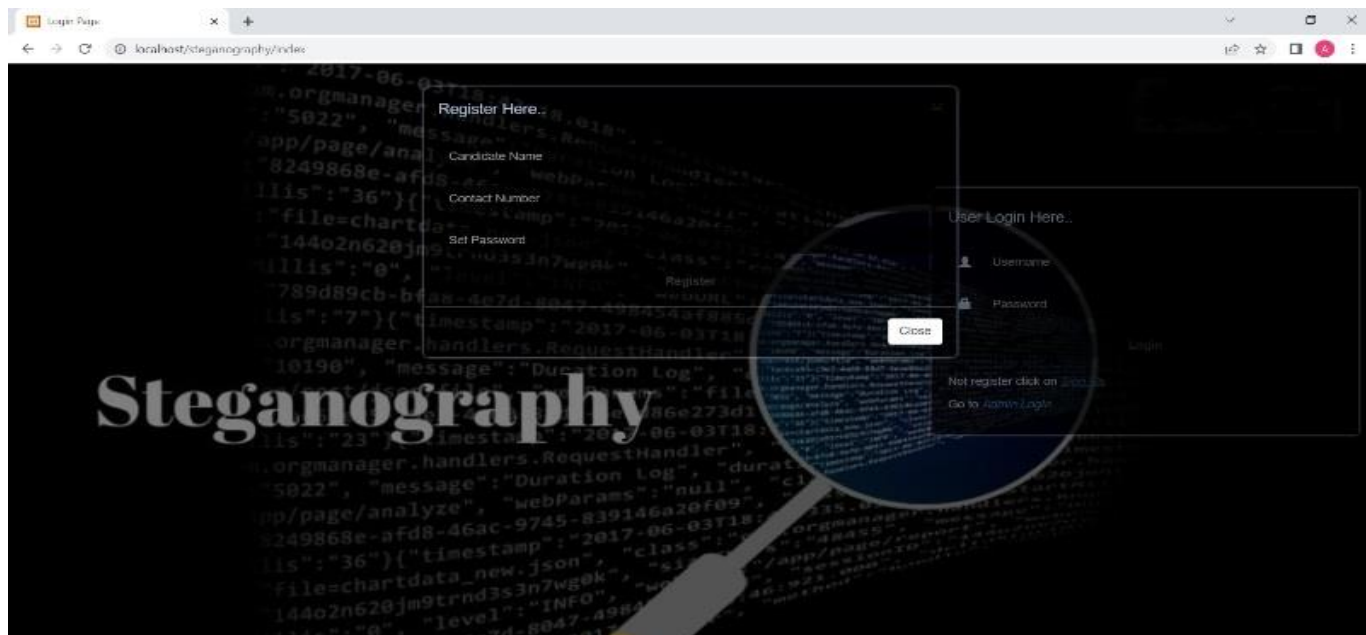


fig : User registration page.

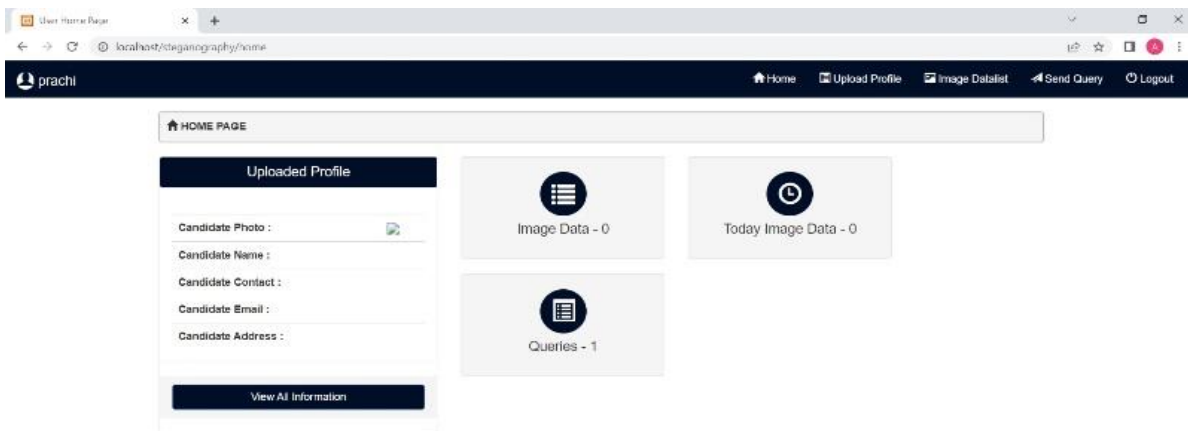


fig: Admin can see , what are the queries of the user

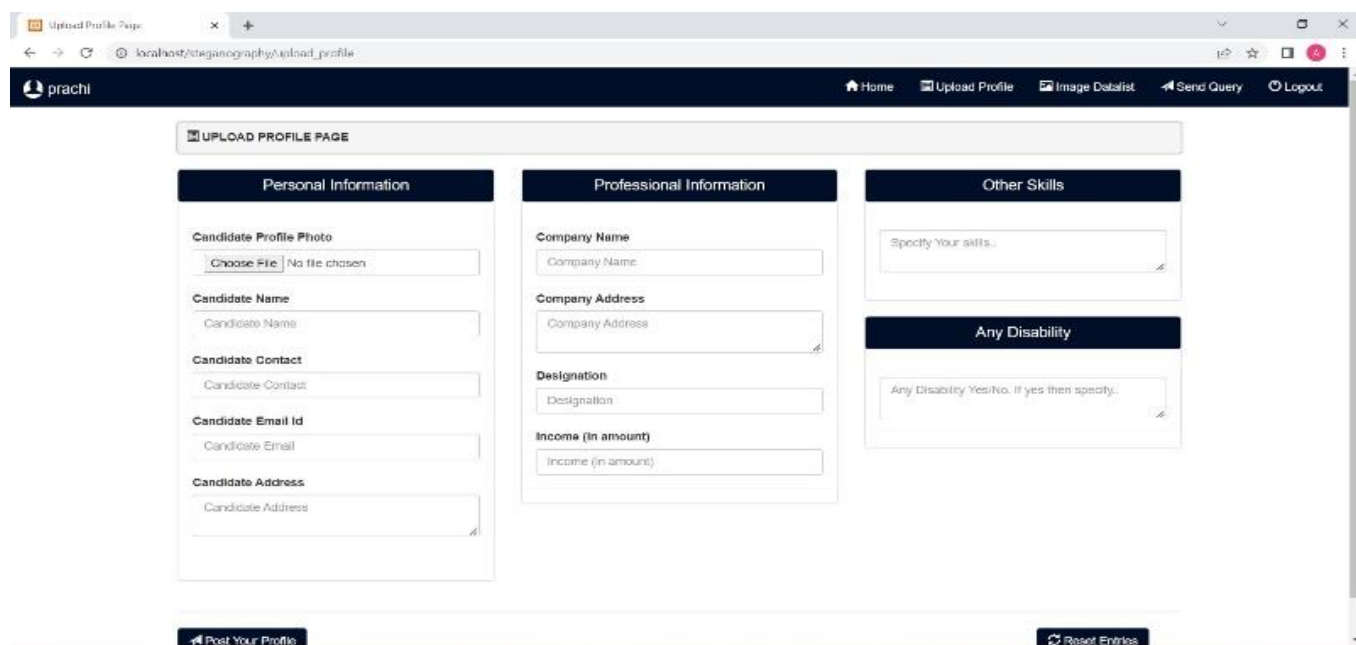


Fig: Shows User can send any data and Query

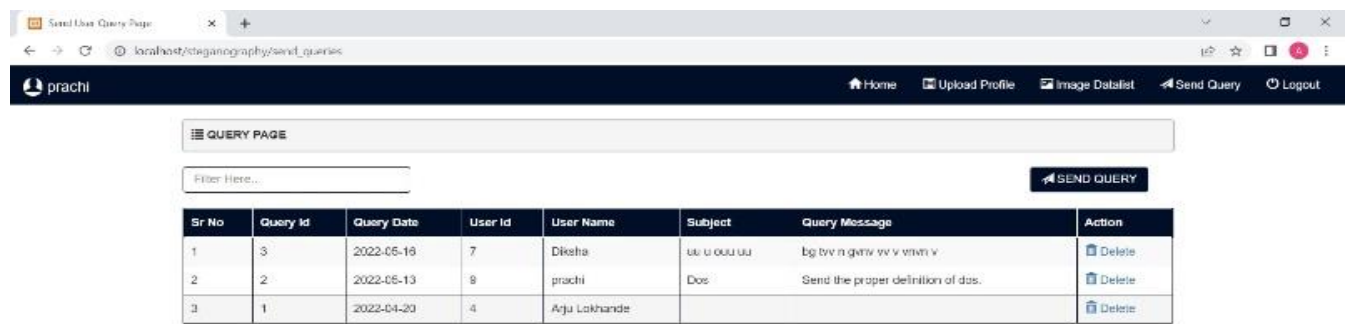


Fig: Query page.

TECHNICAL PAPER

4.1 REVIEW PAPER:

4.1.1 IMPLEMENTATION PAPER:

A Review on Image Steganography using k means and Encryption Techniques

Arju Lokhande[1], Diksha Shelke[2], Prachi pagare[3], Pooja Jawade[4], Ms. Kalpana Bhure[5]

[1],[2],[3],[4] (Department of Computer science and Engineering Jhulelal Institute of Technology, Nagpur, Maharashtra, India)

[5] Assistant Professor, Department of Department of Computer science and Engineering Jhulelal Institute of Technology, 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

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,

I. Introduction

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.

II. 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 digital signal 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 private keys. 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 in MATLAB Using Encrypted Secret Message, Agniswar Dutta, Abhirup Kumar Sen, 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 principle it will be difficult for anyone to decrypt the encrypted message without knowing the exact encryption method. 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 message first and then encrypt it and then finally embed inside the cover file.

[3] Implementation and Comparison of different Data Hiding Techniques in Image Steganography Asha Ashok Poornima 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 the best available locking solution and all tested lock free solutions. We

discussed the relevance of this work and its 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 existing and future scientific and systems applications, which are predominantly in C/C++.

[4] Steganography Based Data Hiding for Security Applications 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-based steganography 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 on for security purposes.

[5] Hiding The Text into An Image By Max-Plus Algebra Kiswara Agung Santoso; Ahmad Kamsyakawuni; 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 of 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 better one among them. PVD substitution on the other hand provides better imperceptibility but is more complex than LSB substitution based on similarity of bit pairs.

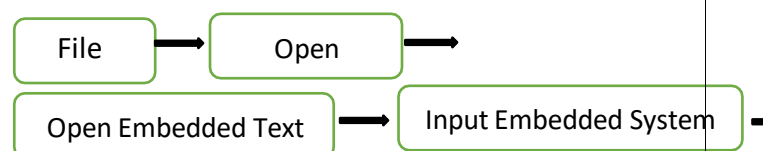
[6] A Novel Approach to Hide Text Data in Color Image, Suraj Kumar; Santosh Kumar; Neeraj Kumar Singh; Anandapra Majumder The

proposed method in the paper, selectively feeds the pixels with secret data. The noise level hence obtained is 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, however small, detected by the steganalysis algorithm is more likely to be overlooked on the account of the transmission channel noise.

I. 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 friendly 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:



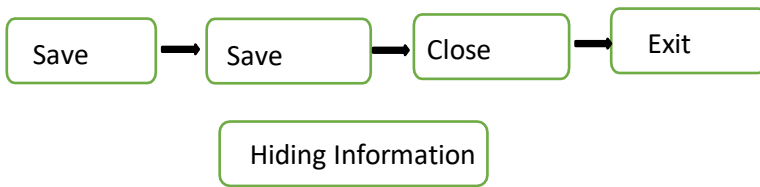


Fig. structure of the proposed system

III. 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.

I. 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.

IV. 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).

4.1.1 IMPLEMENTATION PAPER:

Securing Data Using Image Steganography and Encryption Techniques

Ms.Kalpana Bhure^[1], Araj Lokhande^[2], Diksha Shelke^[3],Prachi pagare^[4],Pooja Jawade^[5]

[1],[2],[3],[4] (Department of Computer science and Engineering Jhulelal Institute of Technology, Nagpur, Maharashtra, India)

[5] Assistant Professor, Department of Department of Computer science and Engineering Jhulelal Institute of Technology, 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 Securing Data using Image Steganography and Encryption technique Steganography is defined as the study of invisible communication. Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The three most important parameters for audio steganography are imperceptibility, payload, and robustness. Different applications have different requirements of the steganography technique used. This paper intends to give an overview of image steganography, its uses and techniques

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

I. INTRODUCTION:

Security of information becomes one of the most important factors of information technology and communication because of the huge rise of the World Wide Web and the copyrights laws. Cryptography was originated as a technique for securing the confidentiality of information. Unfortunately, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret and the concept responsible for this is called

steganography. Steganography is the practice of hiding secret message within any media. Most data hiding systems take advantage of human perceptual weaknesses. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. If both the techniques: cryptography and steganography is used then the communication becomes double secured. The main difference between Steganography and cryptography is that, cryptography concentrates on keeping the contents of a message secret while steganography concentrates on keeping the existence of a message secret. Steganography and cryptography are both needed to protect messages from third party but each one with its own. Thus, when there is a need protect the presence of message; the steganography is the solution. Probably most common cover media are multimedia objects which are images, audio, and video. Here, in this paper, we focus on images as cover media. Two other technologies that are closely related to steganography are watermarking and fingerprinting These technologies are mainly concerned with the protection of intellectual property. Examples of common application of steganography are in the field of copyright protection. According to the information hidden in the bit stream allows an early resynchronization of the video. The only price to pay is a small degradation of the undamaged video quality, with a very limited increase in computational complexity

II. LITERATURE REVIEW

[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 digital signal 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 private keys. 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 in MATLAB Using Encrypted Secret Message, Agniswar Dutta, Abhirup Kumar Sen, 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 principle it will be difficult for anyone to decrypt the encrypted message without knowing the exact encryption method. 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 message first

and then encrypt it and then finally embed inside the cover file.

[3] Implementation and Comparison of different Data Hiding Techniques in Image Steganography Asha Asok Poornima 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 the best available locking solution and all tested lock free solutions. We discussed the relevance of this work and its 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 existing and future scientific and systems applications, which are predominantly in C/C++.

[4] Steganography Based Data Hiding for Security Applications 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-based steganography 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 on for 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 LSBSubstitution with some amount of encryption is the better one 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 to Hide Text Data in Color Image, Suraj Kumar; Santosh Kumar; Neeraj Kumar Singh; Anandapra Majumder The proposed method in the paper, selectively feeds the pixels with secret data. The noise hence obtained is 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, however small, detected by the steganalysis algorithm is more likely to be overlooked on the account of the transmission channel noise.

III. 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 friendly 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:

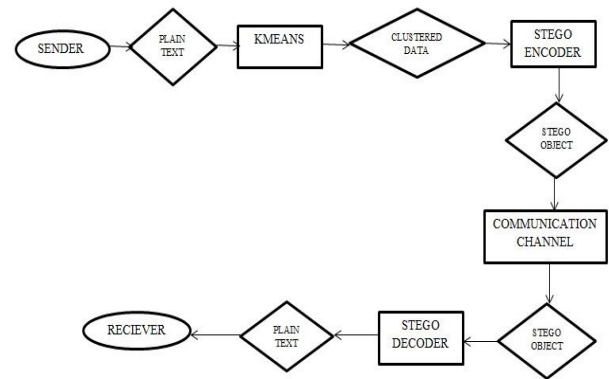


Fig. Proposed Design

IV. MODULES:

- Cluster
- Cluster classification
- Hide-Here the secret message is hidden in image by segmenting the image. Here, K-means clustering technique is used to get accurate results

CLUSTERING:

To create clusters from the input data, we have used k-means clustering algorithm. K-means is one of the simplest unsupervised learning algorithms that solve the well-known clustering

problem. The algorithm initially have empty set of clusters and updates it as proceeds. For each record it computes the Euclidean distance between it and each of the centroids of the clusters. The instance is placed in the cluster from which it has shortest distance. Assume we have fixed metric M , and constant cluster Width W . Let $d_i(C, d)$ is the distance with metric M , Cluster centroid C and instance d where centroid of cluster is the instance from feature vector.

CLUSTER CLASSIFICATION

If cluster width is chosen properly then after clustering each cluster contains instance of same type. The major task is to determine which clusters are normal and intrusive in case of intrusion detection. Here we assume that maximum numbers of records are normal from the training set. Then it is highly possible that the cluster with maximum numbers of instances contains normal records and other contains attack records. We have used 75% as threshold percentage value for labelling the normal cluster. The other clusters are labelled as anomalous

HIDE

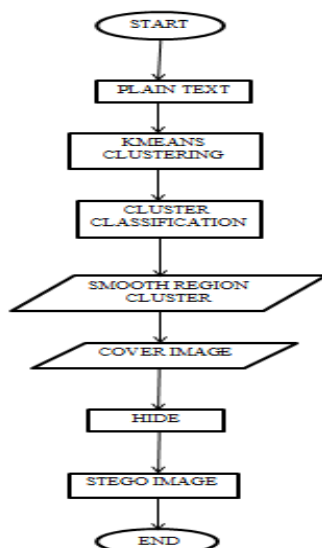


Fig. Encoding Phase

V. IMPLEMENTATION

Steganography is classified among the foremost methods employed in data security to conceal and safeguard confidential messages in the data transmitted. Security, especially data security, is an important requisite in today's world hence Steganography has great significance. The paper deals with understanding and implementation of steganography on different images using two different techniques: Least Significant Bit method (secret image is hidden using the bits at least significant level of the cover image) and Discrete Wavelet Transform method (secret image is hidden by modification of the wavelet coefficients of cover image). The image to be transmitted secretly is both encoded and decoded using these methods and a detailed analysis of the resultant images is performed using various image parameters. These experimentally obtained and compared efficiency parameters, thus, demonstrate the efficiency of the methodology proposed in the paper.

VI. METHODOLOGY

Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. This is a process, which can be used for example by civil rights organizations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to

protect the courier. The initial aim of this study was to investigate steganography and how it is implemented. Based on this work a number of common methods of steganography could then be implemented and evaluated. The strengths and weaknesses of the chosen methods can then be analysed. To provide a common frame of reference all of the steganography methods implemented and analysed used GIF images. Seven steganography methods were implemented. The methods were chosen for their different strengths in terms of resistance to different types of steganalysis or their ability to maximise the size of the message they could store. All of the methods used were based on the manipulation of the least significant bits of pixel values or the rearrangement of color's to create least significant bit or parity patterns, which correspond to the message being hidden.

VII. RESULT ANALYSIS

Admin Page: In Admin Page, Admin login on this page and see the details of Users. Admin can see How many users have registered, what are the queries of the user etc.

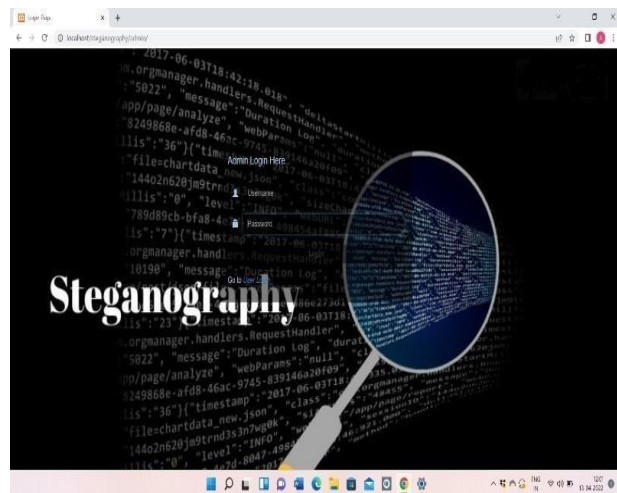
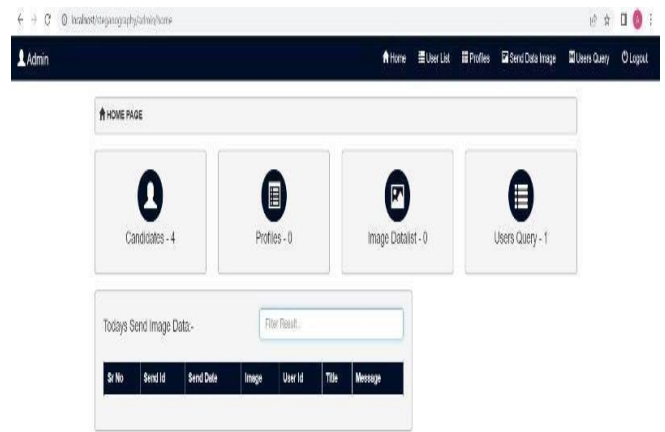


Fig. Admin login page



User Page: In User Page, First User will register on this Page then User will login and fill Complete information. User can send any data; this data will be hidden behind the image. If the user wants to send a query to the admin, the user can Send the query.

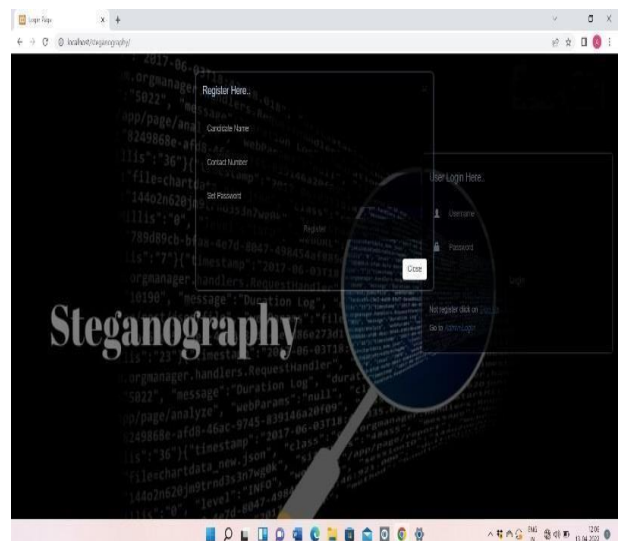
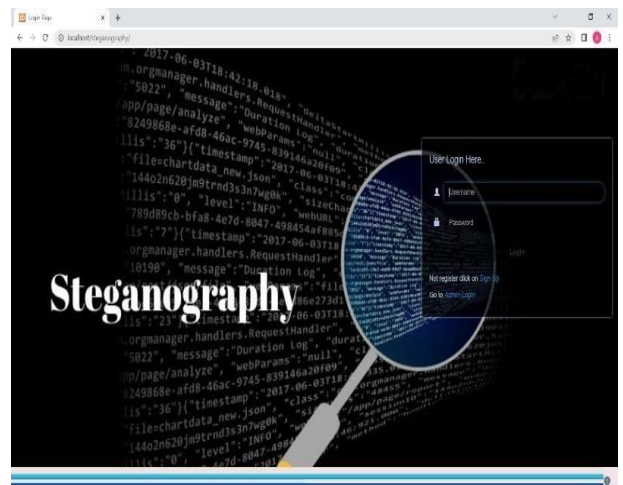


Fig. User registration page

The top screenshot displays the 'User registration page' with the following fields:

- Personal Information:** Candidate Profile Photo (Choose File), Candidate Name, Candidate Contact, Candidate Email Id, Candidate Address.
- Professional Information:** Company Name, Company Address, Designation, Income (in amount).
- Other Skills:** Specify your skills, Any Disability (Any Disability? Yes/No, If yes then specify).

The bottom screenshot shows the 'Admin' dashboard with a sidebar for user management and a main area displaying statistics:

- Uploaded Profile
- Candidate Photo
- Candidate Name
- Candidate Contact
- Candidate Email
- Candidate Address
- View All Information
- Image Data - 0
- Today Image Data - 0
- Queries - 0

Fig. Admin can see what are the queries of the user

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

REFERENCE

- [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)

