PROJECT REPORT ON

Image Steganography using LSB

Submitted by
Shaik. Moinuddin Chisty (ST#IS#4833)

Under the Supervision of

P.V.N

Raghavendra

Senior Security Analyst

Registered And Head
Office D.NO:11-9-
18,1st Floor,
MajjivariStreet,Kothapeta,Vijayawada –520001
+91 9550055338 /+91 7901336873
contact@suprajatechnologies.com

COMPANY PROFILE

Dear Sir/Madam,

We are pleased to inform you that Supraja Technologies is offering Trainings in various domains especially like

- **Ethical Hacking & Cyber Security**
- **Cyber Forensics**
- **IOT Security**

Training plays an important role in the curriculum of a student, it plays very crucialrole in upcoming career aspect of the students as it provides them the gist of the industry in which theywant to opt for. There are too many segments or sectors where students can go for. However, there is apre requisite of having appropriate skill set and thorough knowledge about the relevant technologywhich can help them to enter into the industry. Due to an increase in the number of skilled unemployed and cut throat competition in the jobmarket today, industry demands quiet efficient and more skilled manpower. And this competition hascreated the demand for industrial exposure and industry based support to the student in their coursecurriculum itself.

Supraja Technologies is continuously putting its efforts to fulfil this demand and supply gap
between the industry and institutes with the help of different types of course content for students. Ourextensive R&D based course module helps students out in understanding these new and upcomingtechnologies as per industry norms and impart practical exposure in them so that they can get readyfor tomorrow and make their career in respective segment itself.

COMPANY INTRODUCTION:

Supraja Technologies is a leading Knowledge and Technical Solutions Provider and pioneer leader inIT industry, is operating based out of Vijayawada, Guntur, Visakhapatnam, Hyderabad and Bangalore.

R&D at Supraja

With a 24X7 work in Research& Development, experts at Supraja Technologies work under:

•**Cyber Security Cell**

About Supraja Technologies:

Supraja Technologies (a unit of CHSMRLSS TechnologiesPvt. Ltd.) with its foundation pillars as Innovation, Information and Intelligence is exploring indefinitely as a **Technology Service Provider** and as a**Training Organization**aswell.

You may visit us at:
www.suprajatechnologies.com

The multi domains of trainings which Supraja Technologies operate include the following:

•**Workshops &Hackathons**
○Engineering Colleges
○Schools
○Corporate (Private &Govt)

•**Classroom Trainings Cum Certification Courses**
○Summer Training (30-45 Days)
○Winter Training (10 - 15 Days)
○Weekend Training (2 Days)
○1 Month / 3 Months / 6 Months Courses

•**On-site Trainings**
○College Summer Training (15 Days, 30 Days, 45 Days& 60 Days)
○School Summer Camp (15 Days& 30 Days)
○Govt Agencies, Police Academies, Corporates

•Cloud Campus
○(Distance Learning Program) *Coming Soon

•Internships
○Internship for Engineering Students (15 Days, 30 Days, 45 Days& 60 Days)
○Internship for Graduates (15 Days, 30 Days, 45 Days& 60 Days)

•Lab Setup
○Cyber Lab

Why Supraja Technologies:

Be it Training or a workshop, the course content is alwaysfrom R&D Cell of Supraja.

- A proven track record of delivering quality services.
- **68,500+** Students trained by our trainers till date.
- Training Partners of recognized institutions.
- Trainers with excellent research aptitude and teaching pedagogy illustrate their findings through **practical demonstrations** during their sessions.
- Easy to learn and **hands-on sessions** are given, with additional benefits of Study Material, Tool kit DVD's and immediate query handling.
- Self-Prepared**Cyber Security Cell.**
- Supraja Technologies has the best, experienced and highly **skilled bunch of R&D Engineers & Trainers.**
- We provide training in Innovating and Trending Technologies to Govt. Officials, Corporate Houses and Colleges.

✓ Something we are proud of :

1. Supraja Technologies CEO Mr.SantoshChaluvadi is an Alumni of PottiSriramuluChalavadiMallikharjuna Rao College of Engineering and Technology, Vijayawada.

With our CEO this college conducted/organised a 50hours Nonstop Marathon TrainingWorkshop on Ethical Hacking & Cyber Security for which this respective college and our CEO both holds theirname in **“LIMCA BOOK OF RECORDS 2017”**

2. We are very happy to inform you all that our company, Supraja Technologies has been shortlisted for **"Top 50 Tech Companies" award 2019**, conferred at InterCon - Dubai, UAE.

   Supraja Technologies is one out of thousands companies that were initially screened by InterCon team of 45+ research analysts over a period of three months and the final shortlist includes 150+ firms and we are very proud to inform you all that our company Supraja Technologies also happens to be a part of the same.

✓ Life changing solution/service :

After working on R&D for around 2 years, finally in the mid 2019 we have successfully developed a service/solution of various techniques and strategies for the Film Industry through which he can kill piracy of any film in online up to 25% rightnow. This betaservice is being appreciated & adopted by various Tollywood Film Industry Producers & Hero’s to safeguard their film from piracy in online and to gain more profits.

By the end of 20230 our vision is to rollout a complete full packed service/solution where we can kill piracy entirely 100% everywhere in online for sure.

Apprecation:

Received a great appreciation from our 1stTollywood Film Industry client Mr.Saptagiri for providing our Anti-Piracy betaservice for his filmVAJRA KAVACHADARA GOVINDA

Thanks & Regards,

SANTOSH CHALUVADI
Founder & CEO
+91 – 95500 55338 (M), +91 – 79013 36873 (O)
santosh@suprajatechnologies.com
www.suprajatechnologies.com

Santosh Chaluvadi

Founder & CEO
Supraja Technologies

He is a 27-year-old entrepreneur, one of the India's efficient Cyber Security Analyst and also he is an expert Digital Marketer as well. He is a digital marketer by profession and security enthusiast by passion. He primarily focuses on content building, testing and monetization of blogs. He has successfully developed many websites and done the security testing himself to ensure that the user's data is in safe hands and their privacy is protected. He is very active on social media and shares lot of tech stuff with his followers. The young student hacker has solved many issues with the vulnerabilities present in various websites and databases, given a solution in clearing the loopholes in order to protect the data to be leaked from the databases. Besides Ethical Hacking & Cyber Security, he also has a passion in Blogging & Digital Marketing.

While pursuing his engineering itself, he has trained many young generation people/students of more than 3500+ from various parts across Andhra Pradesh through his workshops, seminars, courses in Cyber Security and this makes him one of the youngest student trainers in India.

At the age of 20 he conducted his first workshop on Blogging & Ethical Hacking which was the beginning to his success in this field and right now he has handful of workshops to train students, government and corporate organizations as well in Andhra Pradesh &Telangana. He is the only student trainer who started conducting workshop for his peers and professors.

❖ Records, Appreciations, Awards & Recognitions etc at a glance :

- ✓ Holds a National Record in **Limca Book of Records – 2017**
- ✓ Steering Committee Member for **United Conference on Cyber Space (UNITEDCON 2020)**
- ✓ Ex-Associate Member for **National Cyber Safety and Security Standards (NCSSS)**
- ✓ Awarded as a **"Karmaveer Chakra - 2019"**, on 12th October 2019 at IIT Delhi, which was instituted by iCONGO in partnership with the United Nations
- ✓ Awarded as a **“Social Media Influencer - 2019”**, on 30th June 2019 byJignasa in association with Government of Andhra Pradesh
- ✓ Nominated for **INDIA 500 CEO AWARD 2019**
- ✓ Invited &**Interviewed by ETV Andhra Pradesh news channel** on 27th July, 2019 for a Special Story Interview on “Spy Apps”
- ✓ **Appreciated by Mr.SridharGaru, Sub-Inspector of Police at Central Crime Branch, Vijayawada** on 23rd October, 2018 for exclusively training him on Special Investigation Course, which will help him to solve the cases easily
- ✓ **Received a great appreciation from our 1stTollywood Film Industry client Mr.Saptagiri,** for providing **Anti-Piracy betaservice** for his movie VAJRA KAVACHADARA GOVINDA

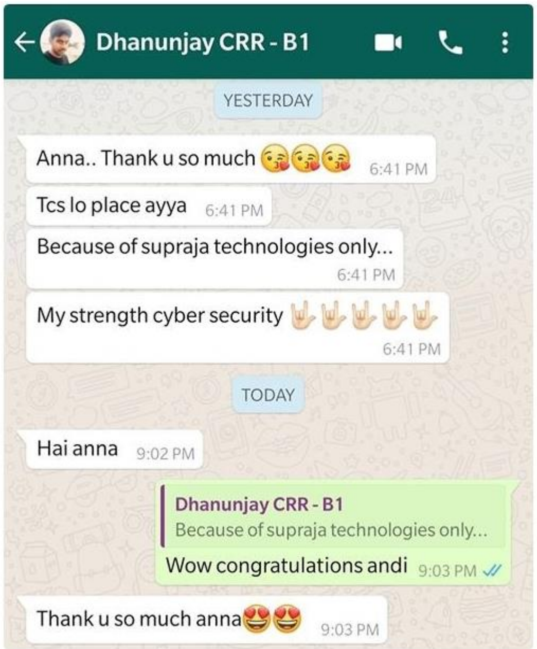
Some Glimpses of our Journey

Mr.SantoshChaluvadi – CEO, Supraja Technologies
Giving hands-on Cyber Security training workshop to the CSE students
at IIT Kharagpur

నయా గూఢచారులుగా మారిన స్మార్ట్‌ఫోన్‌లు
ETV
ఆంధ్ర ప్రదేశ్
సంతోష్, టెక్నాలజీ నిపుణుడు
తాజా
వుపేటలోని అతిథిగృహానికి తరలింపు • సమస్యను నెలలోగా పరిష్కరిస్తామన్న అధి
కర్నూలు
.820
కర్నూలు వ్యవసాయ మార్కెట్‌లో క్వింటాల్

Mr.SantoshChaluvadi – CEO, Supraja Technologies was
Invited & Interviewed by ETV Andhra Pradesh news channel on27th July, 2019
for a Special Story Interview on “Spy Apps”

Mr.SantoshChaluvadi – CEO, Supraja Technologies
Giving Cyber Security training to the students at IIIT Nuzvid



YESTERDAY

Anna.. Thank u so much 😘😘😘 6:41 PM

Tcs lo place ayya 6:41 PM

Because of supraja technologies only... 6:41 PM

My strength cyber security 🤟🤟🤟🤟🤟 6:41 PM

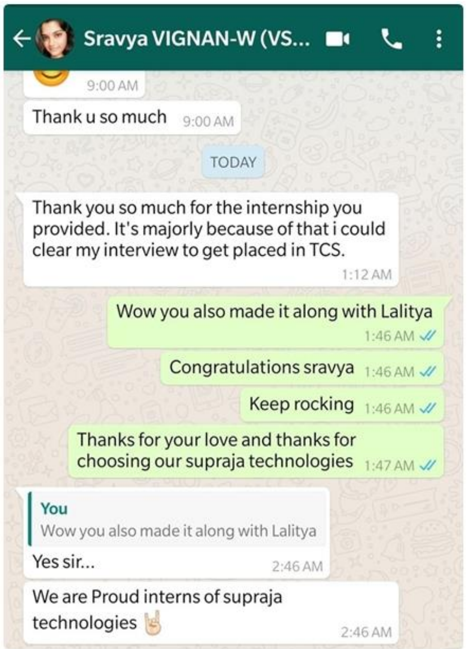
TODAY

Hai anna 9:02 PM

> Dhanunjay CRR - B1
> Because of supraja technologies only...

Wow congratulations andi 9:03 PM

Thank u so much anna😍😍 9:03 PM



9:00 AM

Thank u so much 9:00 AM

TODAY

Thank you so much for the internship you provided. It's majorly because of that i could clear my interview to get placed in TCS. 1:12 AM

Wow you also made it along with Lalitya 1:46 AM

Congratulations sravya 1:46 AM

Keep rocking 1:46 AM

Thanks for your love and thanks for choosing our supraja technologies 1:47 AM

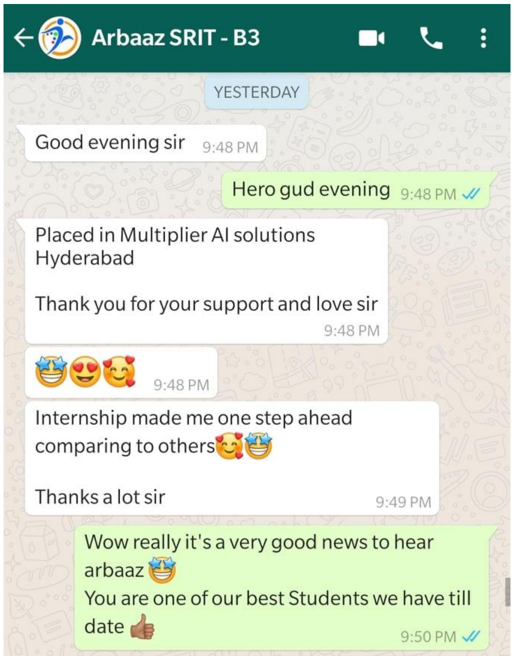
> You
> Wow you also made it along with Lalitya

Yes sir... 2:46 AM

We are Proud interns of supraja technologies 🤘 2:46 AM

In Pictures : Success stories of some of our Internship students of 2019

1. Mr. K Dhanunjay of Sir C R Reddy College Of Engineering, Eluru
2. Ms.SravyaSusarla of Vignan's Institute of Management & Tech for Women, Vizag
3. Mr.ArbaazDilkush Mohammad of SrinivasaRamanujan Institute of Tech, Anantapur



YESTERDAY

Good evening sir 9:48 PM

Hero gud evening 9:48 PM

Placed in Multiplier AI solutions Hyderabad

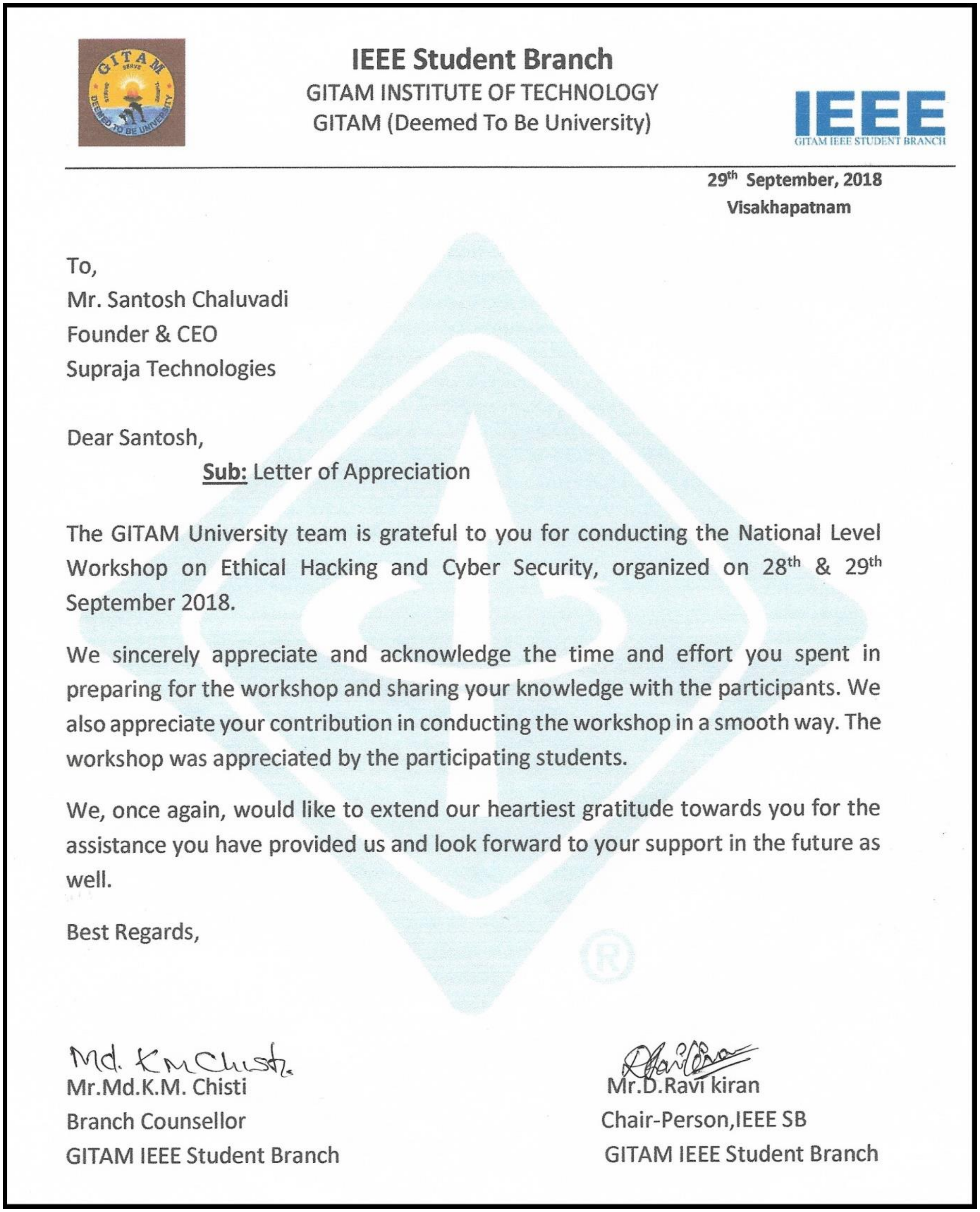
Thank you for your support and love sir 9:48 PM

🤩😍🥰 9:48 PM

Internship made me one step ahead comparing to others🥰🤩

Thanks a lot sir 9:49 PM

Wow really it's a very good news to hear arbaaz🤩
You are one of our best Students we have till date 👍 9:50 PM



IEEE Student Branch
GITAM INSTITUTE OF TECHNOLOGY
GITAM (Deemed To Be University)

IEEE
GITAM IEEE STUDENT BRANCH

29th September, 2018
Visakhapatnam

To,
Mr. Santosh Chaluvadi
Founder & CEO
Supraja Technologies

Dear Santosh,

Sub: Letter of Appreciation

The GITAM University team is grateful to you for conducting the National Level Workshop on Ethical Hacking and Cyber Security, organized on 28th & 29th September 2018.

We sincerely appreciate and acknowledge the time and effort you spent in preparing for the workshop and sharing your knowledge with the participants. We also appreciate your contribution in conducting the workshop in a smooth way. The workshop was appreciated by the participating students.

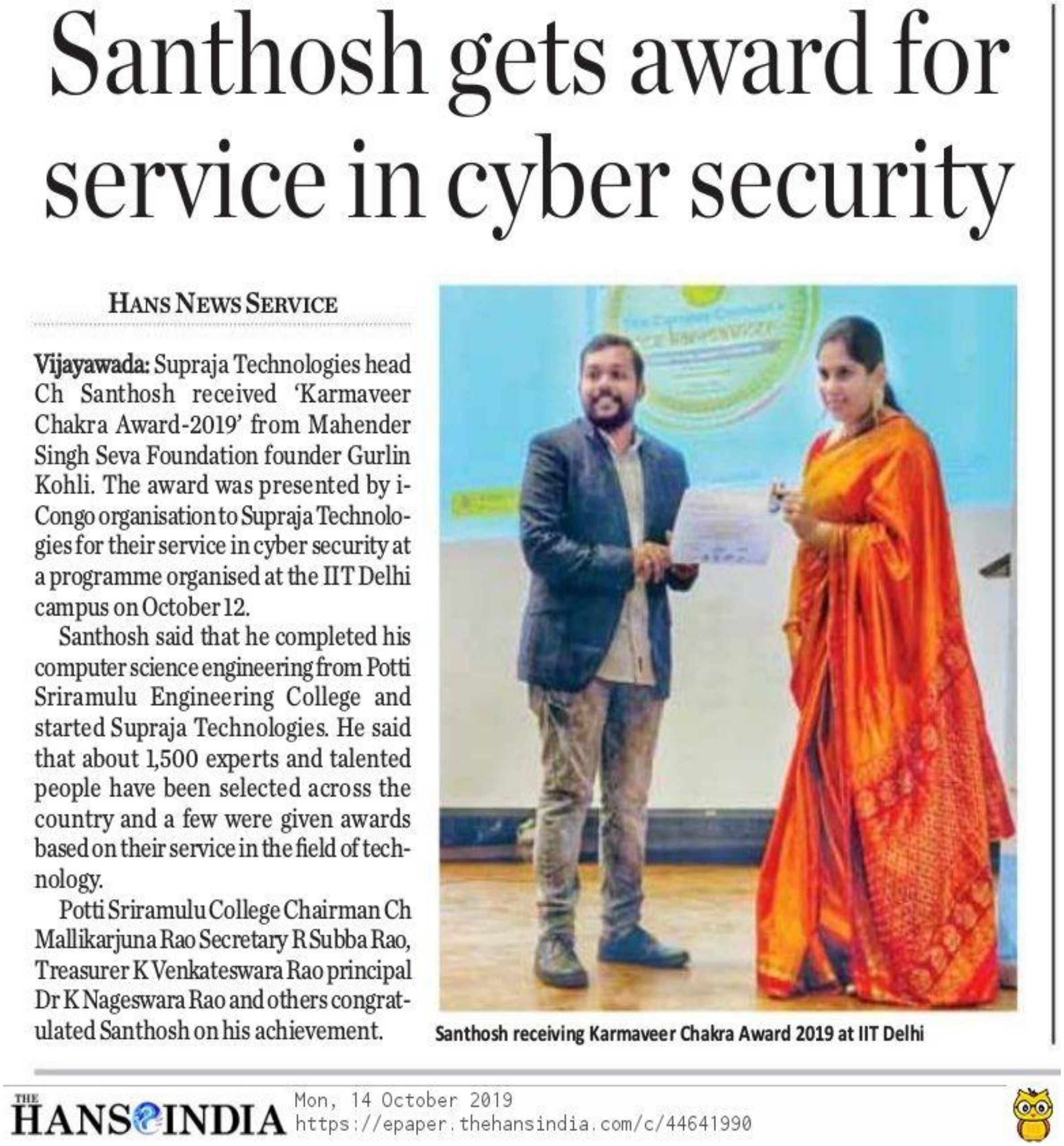
We, once again, would like to extend our heartiest gratitude towards you for the assistance you have provided us and look forward to your support in the future as well.

Best Regards,

Md. KMChisti
Mr.Md.K.M. Chisti
Branch Counsellor
GITAM IEEE Student Branch

Mr.D.Ravi kiran
Chair-Person,IEEE SB
GITAM IEEE Student Branch

Pic Credits : Appreciation from GITAM University, Visakhapatnam



Santhosh gets award for service in cyber security

HANS NEWS SERVICE

Vijayawada: Supraja Technologies head Ch Santhosh received 'Karmaveer Chakra Award-2019' from Mahender Singh Seva Foundation founder Gurlin Kohli. The award was presented by i-Congo organisation to Supraja Technologies for their service in cyber security at a programme organised at the IIT Delhi campus on October 12.

Santhosh said that he completed his computer science engineering from Potti Sriramulu Engineering College and started Supraja Technologies. He said that about 1,500 experts and talented people have been selected across the country and a few were given awards based on their service in the field of technology.

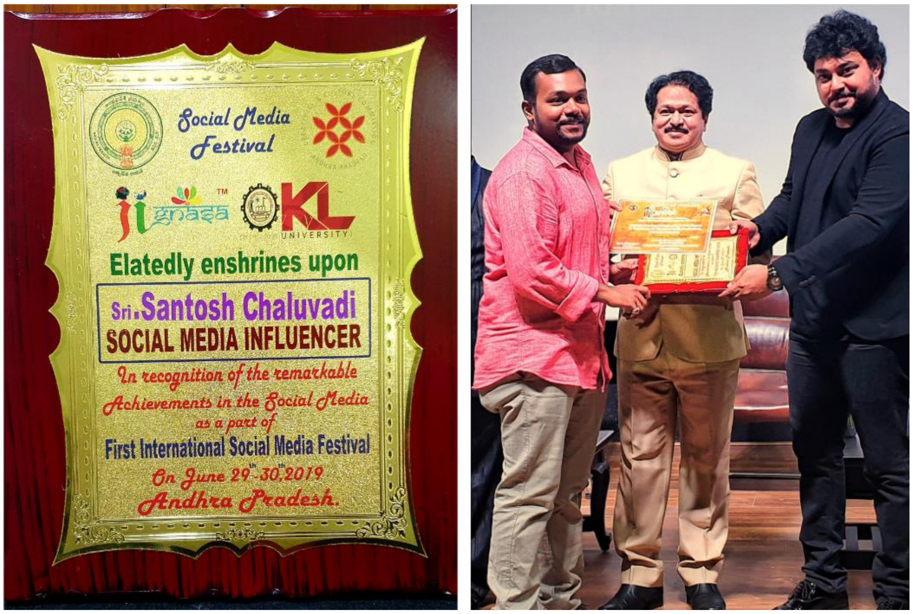
Potti Sriramulu College Chairman Ch Mallikarjuna Rao Secretary R Subba Rao, Treasurer K Venkateswara Rao principal Dr K Nageswara Rao and others congratulated Santhosh on his achievement.

Santhosh receiving Karmaveer Chakra Award 2019 at IIT Delhi

THE HANS INDIA Mon, 14 October 2019
https://epaper.thehansindia.com/c/44641990

Mr. Santosh Chaluvadi, CEO – Supraja Technologies was featured in
THE HANS INDIA newspaper regarding his recently received
"Karmaveer Chakra Award 2019" on October 12th at IIT Delhi,
which was instituted by iCONGO in partnership with the United Nations

Mr.SantoshChaluvadi – CEO, Supraja Technologies gave hands-on Cyber Security training for the students fromDept. of IT at G.Narayanamma Institute of Technology & Science, Hyderabad



Social Media Festival

jignasa™ KL UNIVERSITY

Elatedly enshrines upon

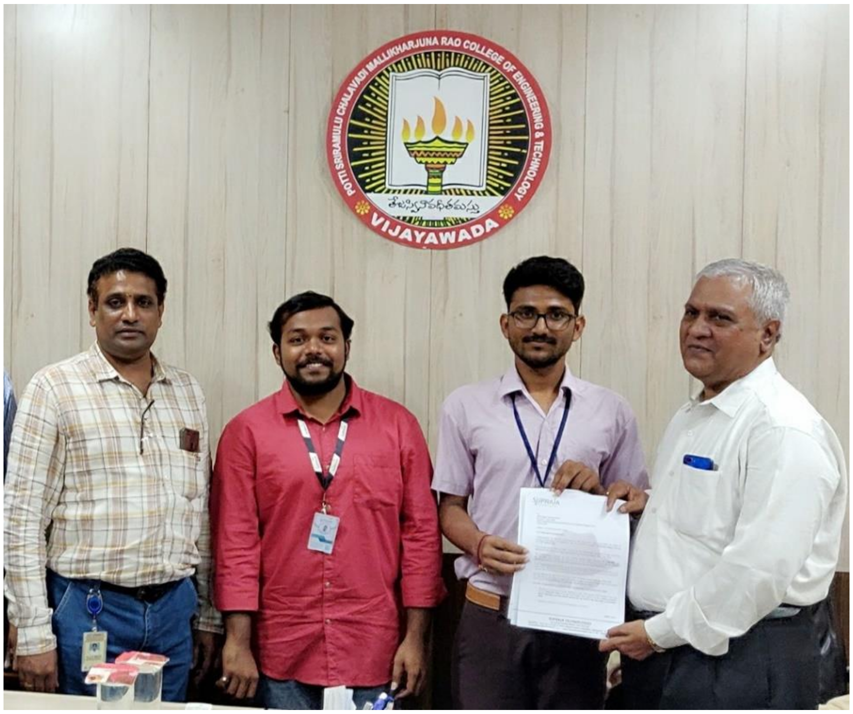
Sri.Santosh Chaluvadi
SOCIAL MEDIA INFLUENCER

In recognition of the remarkable Achievements in the Social Media as a part of
First International Social Media Festival
On June 29th-30th,2019
Andhra Pradesh.

Mr.SantoshChaluvadi – CEO, Supraja Technologies was awarded as a **"Social Media Influencer 2019"** in recognition of his remarkable achievements in the social media as a part of First International Social Media Festival on 30thJune 2019 by Jignasa in association with Government of Andhra Pradesh

Mr.SantoshChaluvadi – CEO, Supraja Technologies
Giving awareness on the latest cyber-attacks to the CSE & IT students at VasireddyVenkatadri Institute of Technology, Guntur

On 23rd October 2018 Mr.SantoshChaluvadi, CEO - Supraja Technologies and Mr.KrishnaChaitanya, CTO - Supraja Technologies has successfully completed delivering Special Investigation Course training in Cyber Security to Mr.SridharGaru, Sub-Inspector of Police at Central Crime Branch, Vijayawada which will help him to solve the cases easily


POTTI SRIRAMULU CHALAVADI MALLIKHARJUNA RAO COLLEGE OF ENGINEERING & TECHNOLOGY
VIJAYAWADA

11th March 2019 is a special day for Mr.SantoshChaluvadi, CEO - Supraja Technologies as he hired a candidate with a salary package of 4.8 LPA from the same college where he studied his engineering ie.,PottiSriramuluChalavadiMallikarjunarao College of Engineering and Technology, Vijayawada

ETV Andhra Pradesh News Channel interviewed Mr.SantoshChaluvadi, CEO - Supraja Technologies for his achievements in the domain of Cyber Security& Digital Marketing

Mr.SantoshChaluvadi – CEO, Supraja Technologies with some of the Internship selected candidates of Supraja Technologies from the Department of IT, Institute of Aeronautical Engineering, Hyderabad

Mr.SantoshChaluvadi – CEO, Supraja Technologies
was felicitated by the department of CSE at St.Mary's Group Of Institutions, Guntur

Supraja Technologies was invited by Indian Air Force (Air Wing NCC) to deliver a session on Latest Cyber Crimes & Awareness for the NCC cadets, staff and officers on 4th July, 2019

Supraja Technologies – CEO, CTO & CMO with
Indian Air Force (Air Wing NCC) Group Captain Sandeep Gupta.
We thank Mr.Sandeep Gupta for inviting us to deliver a session on Latest Cyber Crimes & Awareness for the Indian Air Force (Air Wing NCC) cadets, staff & officers

On 7th March 2019 Mr.SantoshChaluvadi, CEO - Supraja Technologies has hired 4 candidates who has successfully completed their Internship in our Supraja Technologies and finally for their top class performance we appreciated them by offering a pre-placement opportunity in our company

In Picture : Mr.SantoshChaluvadi, CEO - Supraja Technologies along with the Professor, HOD of Computer Science & Engineering and Chairperson, Board of Studies at GITAM University Visakhapatnam,Mr.Thammi Reddy giving away the pre-placement offer letters to the shortlisted candidates of Supraja Technologies

Mr.SantoshChaluvadi along with his Team / Trainers has conducted / organised Workshops, Seminars and Courses on Cyber Security / Ethical Hacking at the following educational institutions and organizations:

- IIT Kharagpur, hosted by AIESEC
- PES University, Bangalore
- GITAM University, Vizag
- CBIT, Hyderabad
- IIIT, Nuzvid
- 2019 Latest Cyber Crimes & Awareness Sessions for the NCC cadets, staff & officers of Indian Air Force (Air Wing NCC)
- Sainik School Korukonda – Under Ministry of Defence
- Vasavi College of Engineering, Hyderabad
- University College of Engineering, Osmania University – Hyderabad
- G. Narayanamma Institute of Technology and Science, Hyderabad
- Institute of Aeronautical Engineering, Hyderabad
- VNR VignanaJyothi Institute of Engineering & Technology, Hyderabad
- Vardhaman College Of Engineering, Hyderabad
- Sreenidhi Institute Of Science & Technology, Hyderabad
- Stanley College of Engineering and Technology for Women, Hyderabad
- University College of Engineering, JNTUK – Vizianagaram
- MVGR College of Engineering, Vizianagaram
- Satya Institute of Technology and Management, Vizianagaram
- Andhra Loyola Engineering College, Vijayawada
- NRI Institute of Technology, Guntur
- St. Mary's Group Of Institutions, Guntur
- Sir C R Reddy College Of Engineering, Eluru
- Eluru College Of Engineering & Technology, Eluru
- Viswanadha Institute of Technology and Management, Vizag
- Raghu Engineering College, Vizag
- Chaitanya Engineering College, Vizag
- Avanthi Institute Of Engineering & Technology, Vizag
- Bomma Institute Of Technology & Science, Khammam
- RISE Group of Institutions, Ongole
- LakkireddyBalireddy College of Engineering, Mylavaram

- DNR Engineering College, Bhimavaram
- GrandhiVaralakshmiVenkata Rao Institute of Technology, Bhimavaram

and many more workshops, corporate trainings, seminars, faculty development programs, one-one sessions, online trainings etc...

Thanks & Regards,

SANTOSH CHALUVADI
Founder & CEO
+91 – 95500 55338 (M), +91 – 79013 36873 (O)
santosh@suprajatechnologies.com
www.suprajatechnologies.com

SUPRAJA TECHNOLOGIES – KEY TRAINER

Krishna Chaitanya

- **Chief Technology Officer**
- **Head - IT Security**
- **Head - Cyber Forensics Investigation**
- **Chief Trainer at Supraja Technologies**

He is a 27 year old passionate, goal-oriented IT professional in Computer Digital Forensics & Ethical Hacking. He is an expert in Vulnerability Assessment and Penetration Testing (VAPT). He holds a responsible and challenging position with a turbulent and dynamic professional development and where he can best utilize his knowledge and skills. He has been assisting for Telangana State Police Academy and various Government Department Officials, Private sector Officials across India.

WHAT I DO : (DIGITAL FORENSICS)

The Advanced Digital Forensics focuses on the entire investigative process, from the very beginning through the conclusion and determination of who did it. Adequate knowledge on Digital Forensics which can drive me to investigate typical Cyber Crimes. Handling incident response and perform analysis to trace out the foot prints.

- Develop an investigative process for the digital forensic investigation
- Understanding methods of focusing investigations through analysis of multiple evidence sources
- Effectively prepare for incident response of both victim and suspect systems, including understanding the importance of network reconnaissance and network traffic analysis
- Identify sources of evidentiary value in various evidence sources including network logs, network traffic, volatile data and through disk forensics
- Identify common areas of malicious software activity and characteristics of various types of malicious software files
- Confidently perform live response in intrusion investigation scenarios
- Recovering data from damaged or erased hard drives.
- Writing, reviewing investigative reports & gathering, maintaining evidences
- Working closely with other police officers and detectives

- Imaging & Hashing

WHAT I DO: (VA&PT)

Analyses and assesses vulnerabilities in the infrastructure (applications & networks), investigates the available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyses and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures may assist in the creation, implementation and/or management of security solutions.

TRAINING :

Now-a-days the demand for Computer Digital Forensics &Ethical Hackers has increased. I used to give training for corporate companies, schools and college students. I used to conduct seminars and workshops for the same. I possess strong background knowledge of Ethical Hacking, Computer Digital Forensics, Networking, Web Applications, Current security protocols for popular operating environments etc.

CERTIFICATIONS, HONORS, APPRECIATIONS, AWARDS & RECOGNITIONS:

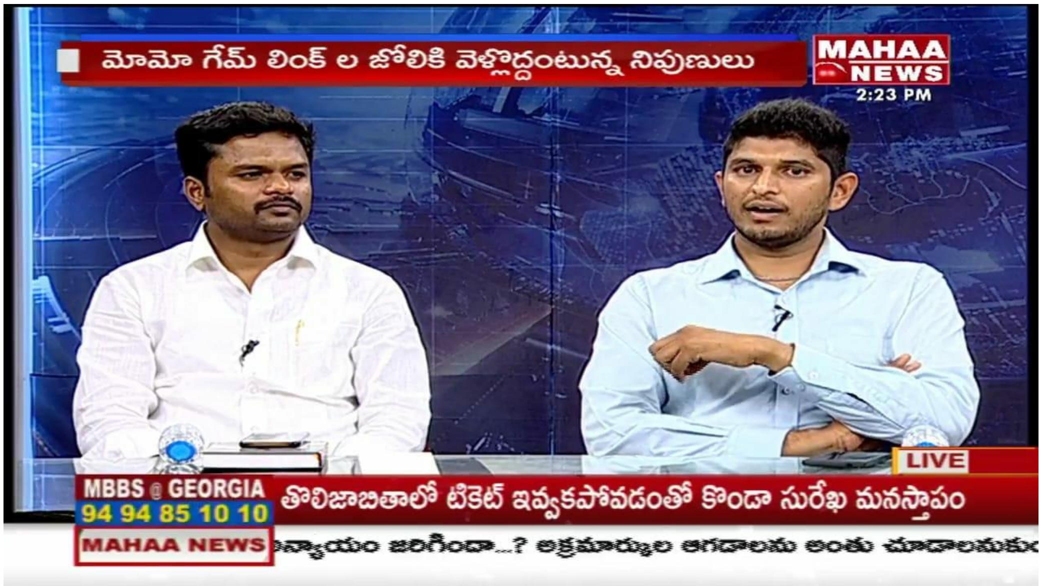
- CPEH : Certified Professional Ethical Hacker
- CPTE : Certified Penetration Testing Engineer
- CHFI : Certified Hacking Forensics Investigator
- RHCE : Red Hat Certified Engineer
- Worked as a core member for National Information Security Summit 2017
- Appreciation from E-HACK
- Appreciation Certification from National Cyber Safety& Security Standards
- Appreciation for finding out Vulnerabilities in websites like Sony, Intel etc
- Appreciation from Telangana State Police Academy for training some of the department officials on various Cyber Attacks
- Honoured & Appreciated from Honourable Member of Parliament and TelanganaRashtraSamithi party member Smt. KalvakuntlaKavithaGaru

- Appreciated by various Universities, College Managements, Organizations and Technocrats
- Invited by Mahaa News channel on Sept 8, 2018 for a Live Debate on Momo Challenge

Mr.KrishnaChaitanya – CTO, Supraja Technologies
Giving training to the department staff at Telangana State Police Academy

Mr.KrishnaChaitanya – CTO, Supraja Technologies
With some of the department officials at Telangana State Police Academy

Mr.KrishnaChaitanya – CTO, Supraja Technologies
Honoured & Appreciated from Honourable Member of Parliament and
TelanganaRashtraSamithi party member Smt. KalvakuntlaKavithaGaru


మోమో గేమ్ లింక్ ల జోలికి వెళ్లొద్దంటున్న నిపుణులు
MAHAA NEWS
2:23 PM
LIVE
MBBS @ GEORGIA
94 94 85 10 10
తొలిజాబితాలో టికెట్ ఇవ్వకపోవడంతో కొండా సురేఖ మనస్తాపం
MAHAA NEWS
న్యాయం జరిగిందా...? అక్రమార్కుల ఆగడాలను అంతు చూడాలనుకు

Mr. Krishna Chaitanya – CTO, Supraja Technologies
Invited by Mahaa News channel @ Sept 8, 2018 for Live Debate on MomoChallenge

Table of Contents

Abstract

Hiding an important message within an image is known as image steganography. Imperceptibility of the message is a major concern of an image steganography scheme. A novel single digit sum (SOS) based image steganography scheme has been proposed in this paper. At first, the computation of SOS has been generalized to support a number system with any given base. Then, an image steganography scheme has been developed, where the base for computing SOS is varied from one pixel to another. Therefore, the number of embedding bits in a pixel is varied across pixels. The purpose of this technique is to control the amount of change in a pixel. A lossy compressed version of the cover image is used to determine the upper limit of change in each pixel value. The base for computing SOS is determined by using this upper limit for a pixel. Thus, it is ensured that the stego image does not degrade beyond the degradation in the lossily compressed image.

Overall Description:

The technique of imperceptibly hiding an important message within a cover image is called image steganography. Only the intended recipients can extract the message from the received image. Others remain unaware of the very presence of this covert communication. Over the years, researchers have come up with novel steganography techniques ensuring imperceptibility and undetectability of the message.

Steganography usually deals with the way to hide the existence of communicated data in such a way that it remains confidential. It maintains secrecy between the two communicating bodies. Secrecy is achieved in the image steganography, by embedded data into the cover images and generating a stego-images.

Introduction:

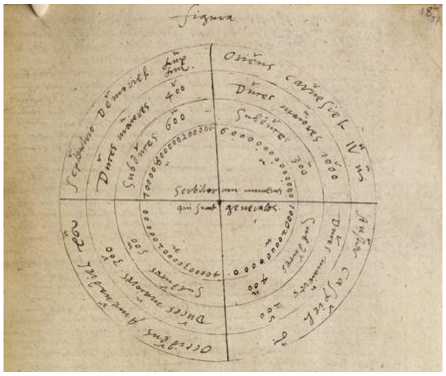
What is Steganography?

The word “**Stegano**” mean “**cover**” and “**Graphical**” mean “**write**”. Thus, Stegano and graph both combine to make the process in which we hide the important information inside the image using some encoding technique. This process not only hides the data it also hides the communication which means others will not know whether the communication is taking place or not. Imagine hiding your secret information in a digital media without scrambling its original contents.

The technique of hiding secret data within an ordinary, non-secret, file, or message in order to avoid detection. Practice of concealing a message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient.

History of Steganography:

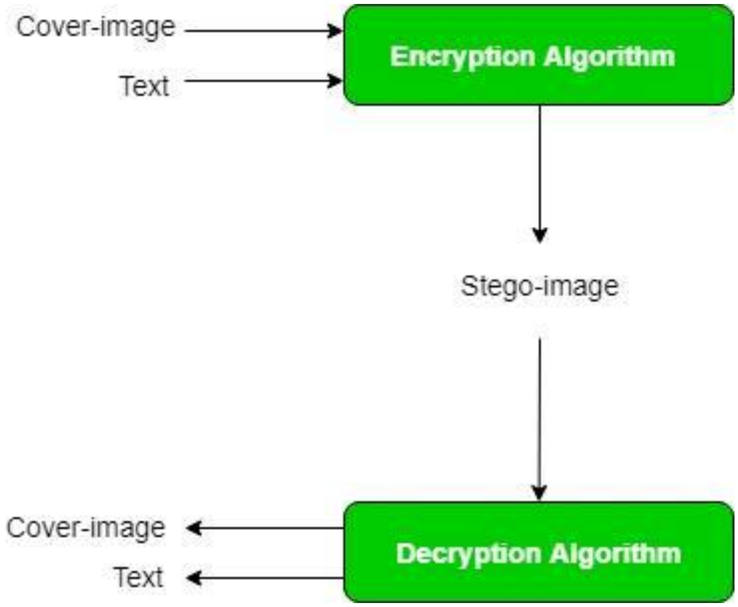
The first recorded uses of steganography can be traced back to 440 BC in Greece, when Herodotus mentions two examples in his histories. Histiaeus sent a message to his vassal.



Steganography is thus an art of covered writing that is not seen by any person other than the intended recipient. Steganography continued development in the early 1600s by Sir Francis Bacon. During times of war, invisible inks were used in steganography extensively. The British and American forces used various forms of Invisible Inks in American Revolutionary War.

Invisible Ink used mainly were milk, vinegar, fruit juice, and urine, for the hidden text. The receiver used heat and light to read or decode them. World War II introduced microdots by the Germans. Null ciphers i.e. unencrypted messages.

The process of Image Steganography



Terminologies:

The payload is the data covertly communicated. The carrier is the signal, stream, or data file that hides the payload, which differs from the channel, which typically means the type of input, such as a JPEG image.

The resulting signal, stream, or data file with the encoded payload is sometimes called the package, stego file, or covert message. The proportion of bytes, samples, or other signal elements modified to encode the payload is called the encoding density and is typically expressed as a number between 0 and 1.

In a set of files, the files that are considered likely to contain a payload are suspects. A suspect identified through some type of statistical analysis can be referred to as a candidate.

APPROACHES USED

LSB (Least Significant Bit): Least critical piece (LSB) is the bit position in a parallel whole number giving the units esteem, that is, deciding if the number is even or odd. The LSB is occasionally alluded to as the right-most piece, because of the tradition in positional documentation of composing less noteworthy digit further to one side. It is like the least critical digit of a decimal whole number, which is the digit during the ones (right-most) situated and Technology.

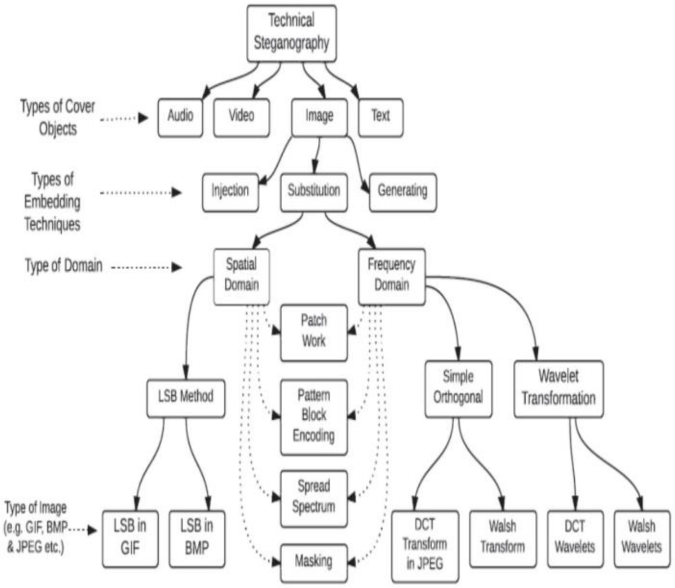
Despite the fact that LSB shrouds the message in such way that the people don't see it, it is as yet feasible for the rival to recover the message because of the effortlessness of the procedure. In this way, malignant individuals can without much of a stretch attempt to remove the message from the earliest starting point of the picture in the event that they are suspicious that there exists mystery data that was inserted in the picture.

Analysis:

Image steganography is the practice of hiding secret data within an image. It is a technique used to protect the confidentiality of data and prevent unauthorized access.Image steganography is most popular form of steganography. Here secret message is embedded into an image as noise, which is nearly impossible to detect by human eyes. Data hiding in still image imposes certain challenges to cope up with human visual systems (HVS).
The process of Image steganography involves embedding the secret data, often referred to as the “payload,” into the pixels of an image. This can be done by

modifying the least significant bits (LSBs) of the image's color channels, such as red, green, and blue (RGB), or by using more complex algorithms that take advantage of the human eye's limited sensitivity to slight changes in color or intensity.

Image steganography can be a valuable tool for certain applications, such as covert communication or digital watermarking, but its implementation should be guided by a thorough understanding of its limitations, potential risks, and compliance with applicable laws and regulations.



Here are some advantages and disadvantages of Image Steganography:

Advantages:

- Provides high level security for data sharing process.
- Doesn't require any additional software in the system.
- Difficult to detect (only receiver can detect).
- Resistance to Attacks: Steganography techniques can offer resistance against certain attacks aimed at compromising data integrity.
- Camouflage and Stealth: Steganography allows information to blend seamlessly with its surroundings.
- Security and Covert Communication: Steganography provides a means of secret communication by hiding sensitive or confidential information.
- Enhanced Data Protection: Steganography can be used to enhance the security of data transmission and storage.

Disadvantages:

- Loss Compression: Steganography can be negatively impacted by loss compression algorithms commonly used in digital media formats such as JPEG for images or MP3 for audio.
- Secret data that can be hidden is limited by size of the image.
- Quality of image maybe compromised due to hidden data.
- It is time consuming.
- Susceptibility to Detection: While steganography aims to hide information, it is not entirely immune to detection.
- Limited Capacity: One of the main disadvantages of steganography is the limited capacity for hiding information within the carrier file.
- Increased Complexity: Implementing steganography techniques can add complexity to systems and workflows.

Applications of Image Steganography:

- It is used in the military and intelligence agencies to protect sensitive information.
- It is used in digital watermarking to protect copyright and ownership of images.
- It is used in the medical field to securely transmit patient information.
- Confidential communication and secret data storing
- Protection of data alteration
- Access control system for digital content distribution
- Media Database systems

DETECTING AN IMAGE STEGANOGRAPHY:

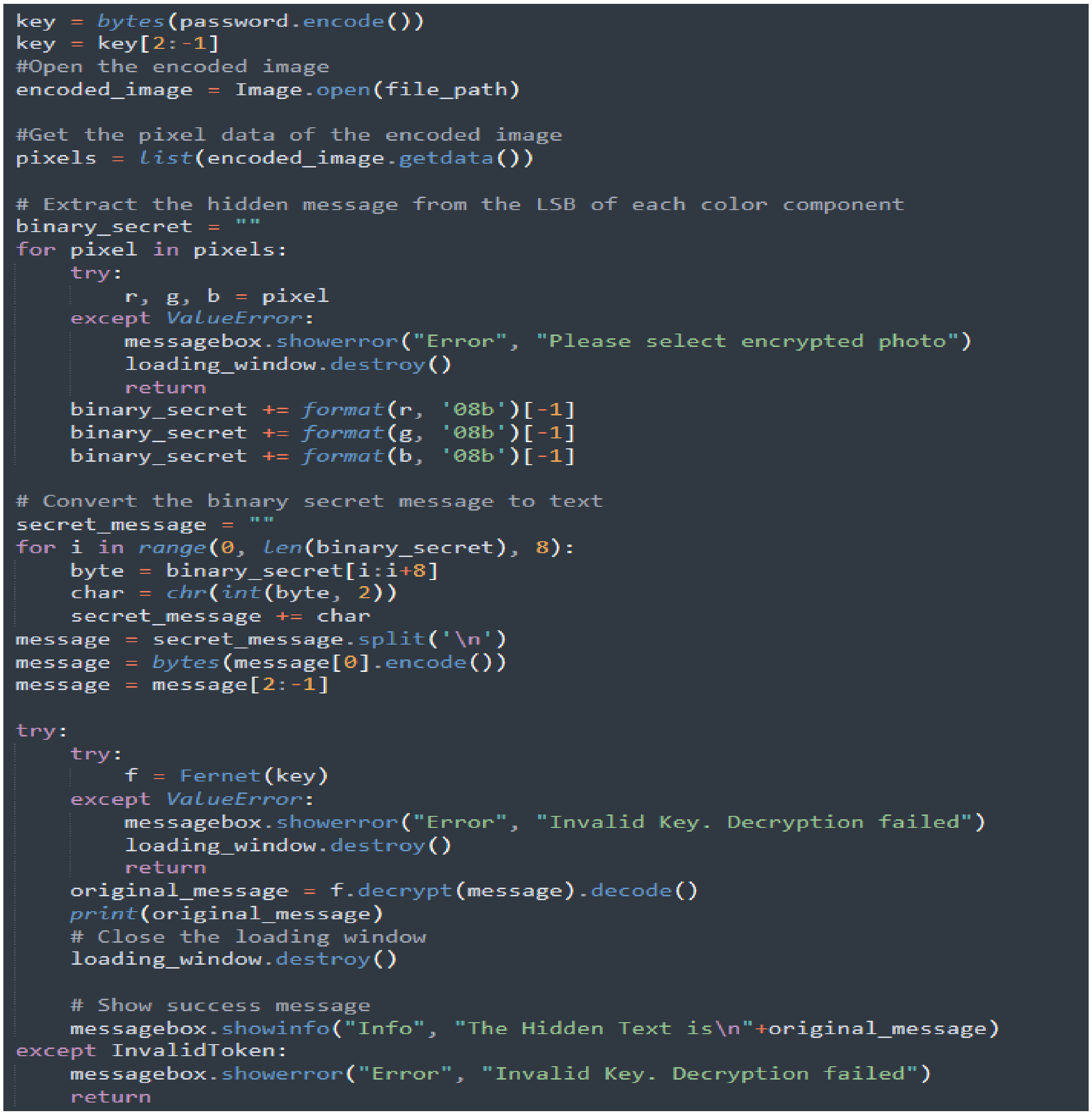
Image analysis techniques such as histogram analysis and visual inspection can be used to detect steganography.Statistical analysis can also be used to detect hidden data by analyzing the distribution of pixel values in the image.Specialized steganography detection tools such as StegAlyzerAS can also be used to detect steganography.

Detecting physical steganography requires a careful physical examination, including the use of magnification, developer chemicals, and ultraviolet light. It is a time-consuming process with obvious resource implications, even in countries that employ many people to spy on their fellow nationals. However, it is feasible to screen mail of certain suspected individuals or institutions, such as prisons or prisoner-of-war (POW) camps.

In computing, steganographically encoded package detection is called steganalysis. The simplest method to detect modified files, however, is to compare them to known originals. There are many techniques known to be able to hide messages in data using steganographic techniques. None are, by definition, obvious when users employ standard applications, but some can be detected by specialist tools.

Design

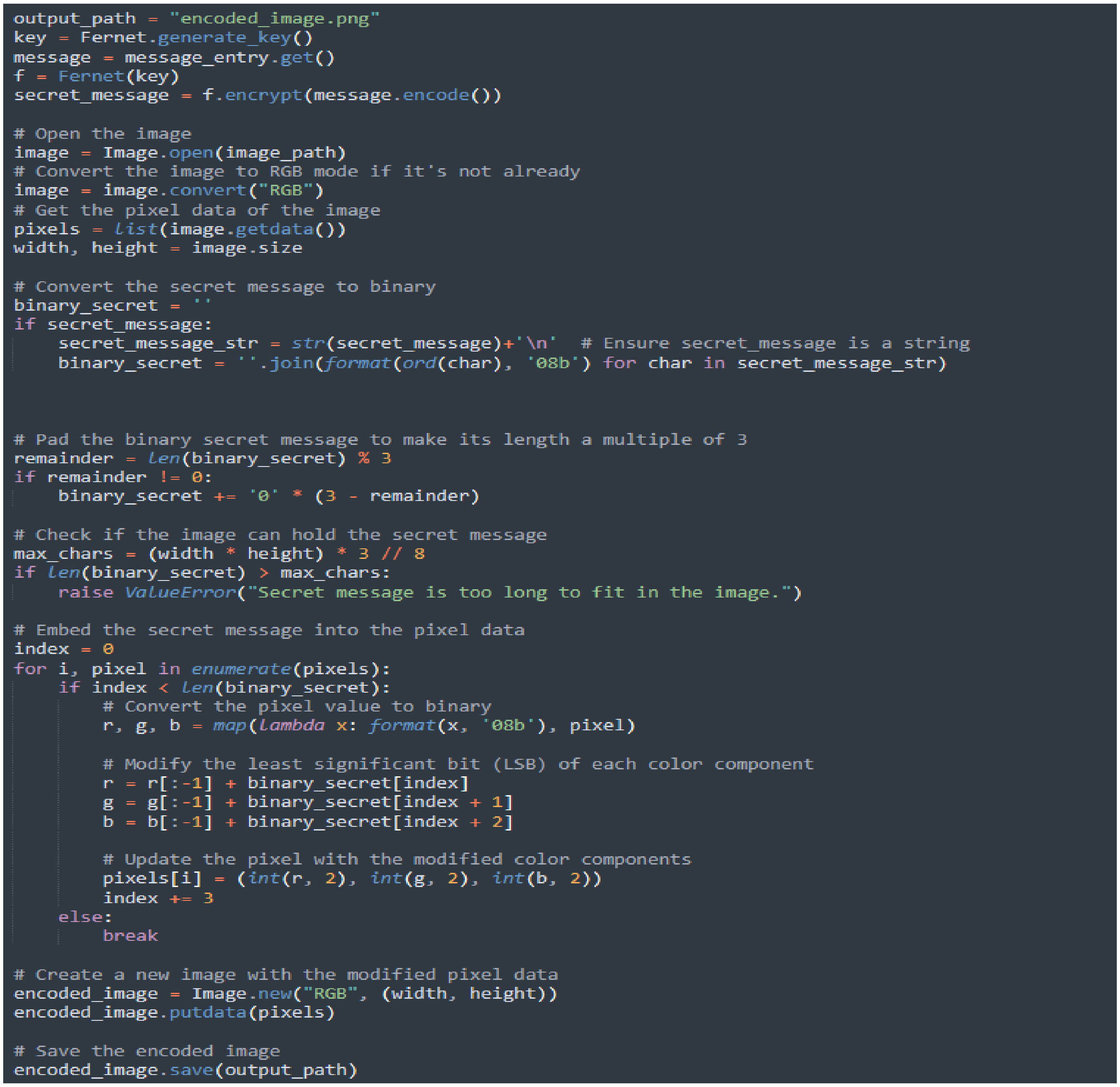
Decoding: Decoding is the process of retrieving the hidden information from a stenographic image. It is the reverse operation of encoding. The decoding algorithm scans the stego-image, analyzes it, and extracts the concealed data.



```
key = bytes(password.encode())
key = key[2:-1]
#Open the encoded image
encoded_image = Image.open(file_path)

#Get the pixel data of the encoded image
pixels = list(encoded_image.getdata())

# Extract the hidden message from the LSB of each color component
binary_secret = ""
for pixel in pixels:
    try:
        r, g, b = pixel
    except ValueError:
        messagebox.showerror("Error", "Please select encrypted photo")
        loading_window.destroy()
        return
    binary_secret += format(r, '08b')[-1]
    binary_secret += format(g, '08b')[-1]
    binary_secret += format(b, '08b')[-1]

# Convert the binary secret message to text
secret_message = ""
for i in range(0, len(binary_secret), 8):
    byte = binary_secret[i:i+8]
    char = chr(int(byte, 2))
    secret_message += char
message = secret_message.split('\n')
message = bytes(message[0].encode())
message = message[2:-1]

try:
    try:
        f = Fernet(key)
    except ValueError:
        messagebox.showerror("Error", "Invalid Key. Decryption failed")
        loading_window.destroy()
        return
    original_message = f.decrypt(message).decode()
    print(original_message)
    # Close the loading window
    loading_window.destroy()

    # Show success message
    messagebox.showinfo("Info", "The Hidden Text is\n"+original_message)
except InvalidToken:
    messagebox.showerror("Error", "Invalid Key. Decryption failed")
    return
```

<u>Encoding:</u> Image steganography is a technique used to hide secret information within an image in such a way that is imperceptible to the human eye and appears like an ordinary image. The encoding process involves embedding the hidden data (message, file, or any other

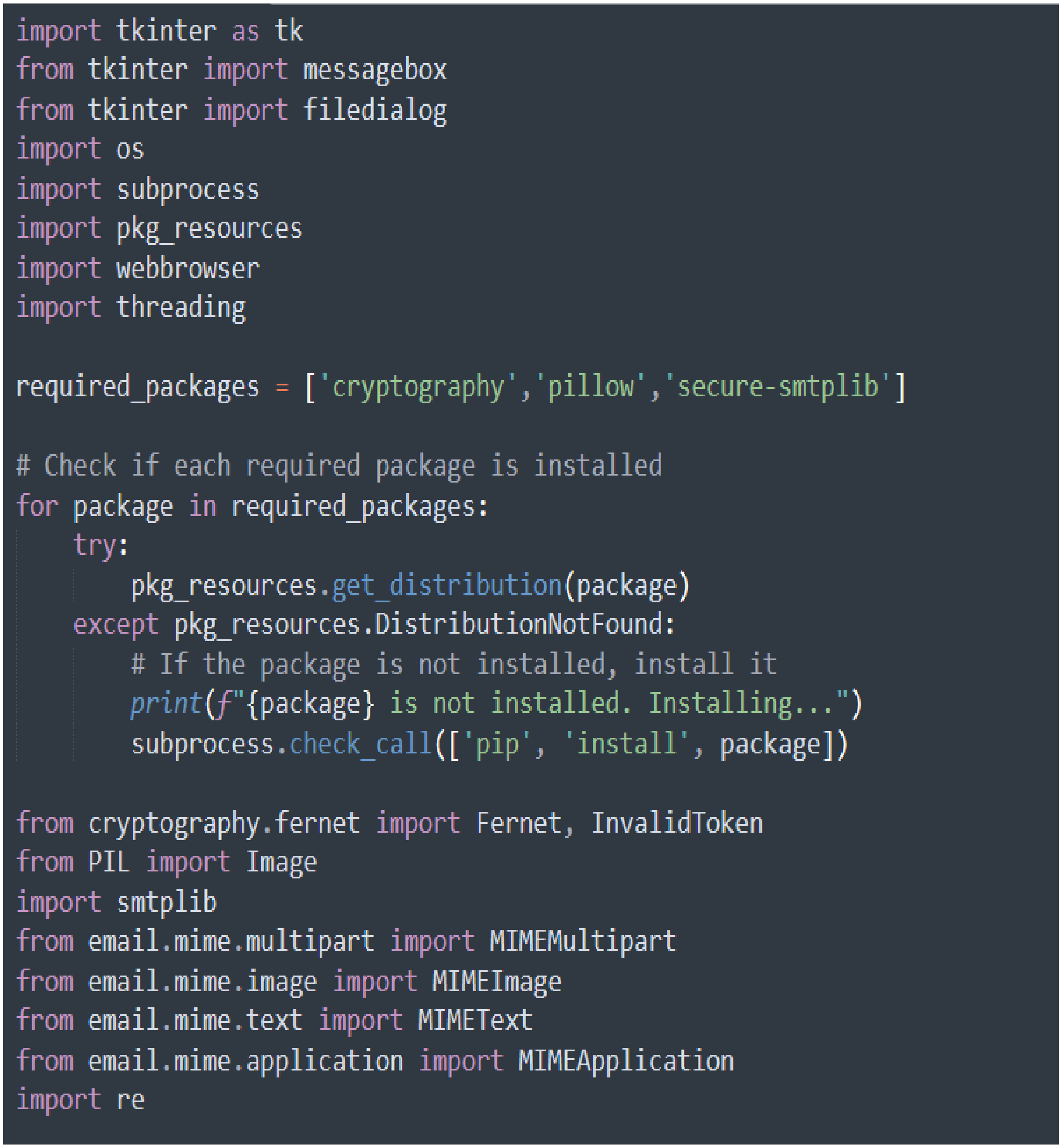
sensitive information) into the pixel values of the image.



```
output_path = "encoded_image.png"
key = Fernet.generate_key()
message = message_entry.get()
f = Fernet(key)
secret_message = f.encrypt(message.encode())

# Open the image
image = Image.open(image_path)
# Convert the image to RGB mode if it's not already
image = image.convert("RGB")
# Get the pixel data of the image
pixels = list(image.getdata())
width, height = image.size

# Convert the secret message to binary
binary_secret = ''
if secret_message:
    secret_message_str = str(secret_message)+'\n'  # Ensure secret_message is a string
    binary_secret = ''.join(format(ord(char), '08b') for char in secret_message_str)



# Pad the binary secret message to make its length a multiple of 3
remainder = len(binary_secret) % 3
if remainder != 0:
    binary_secret += '0' * (3 - remainder)

# Check if the image can hold the secret message
max_chars = (width * height) * 3 // 8
if len(binary_secret) > max_chars:
    raise ValueError("Secret message is too long to fit in the image.")

# Embed the secret message into the pixel data
index = 0
for i, pixel in enumerate(pixels):
    if index < len(binary_secret):
        # Convert the pixel value to binary
        r, g, b = map(lambda x: format(x, '08b'), pixel)

        # Modify the least significant bit (LSB) of each color component
        r = r[:-1] + binary_secret[index]
        g = g[:-1] + binary_secret[index + 1]
        b = b[:-1] + binary_secret[index + 2]

        # Update the pixel with the modified color components
        pixels[i] = (int(r, 2), int(g, 2), int(b, 2))
        index += 3
    else:
        break

# Create a new image with the modified pixel data
encoded_image = Image.new("RGB", (width, height))
encoded_image.putdata(pixels)

# Save the encoded image
encoded_image.save(output_path)
```

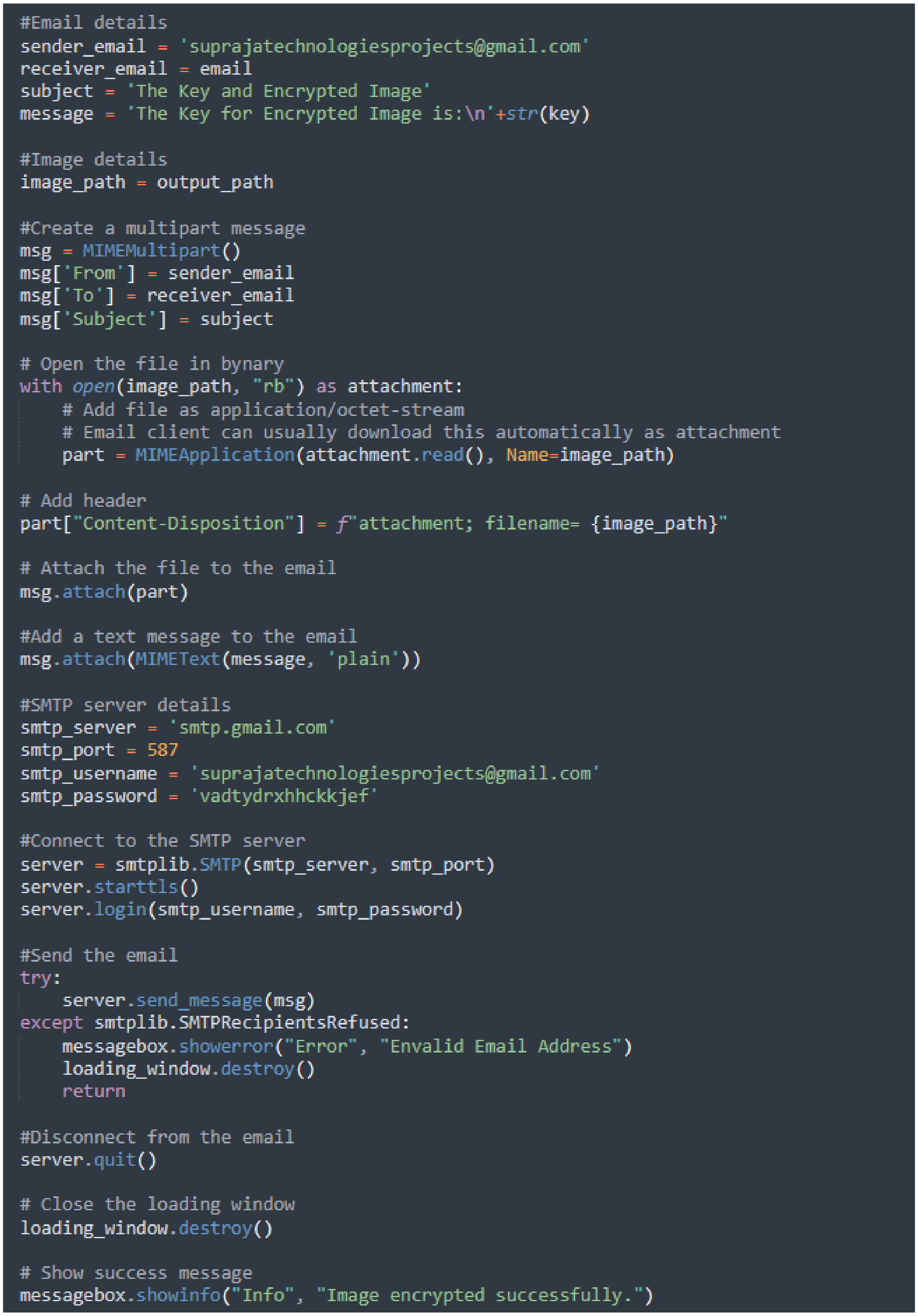
Required packages:

1. **Pillow (PIL Fork)**
2. **NumPy**
3. **Optional: Matplotlib**



```python
import tkinter as tk
from tkinter import messagebox
from tkinter import filedialog
import os
import subprocess
import pkg_resources
import webbrowser
import threading

required_packages = ['cryptography','pillow','secure-smtplib']

# Check if each required package is installed
for package in required_packages:
    try:
        pkg_resources.get_distribution(package)
    except pkg_resources.DistributionNotFound:
        # If the package is not installed, install it
        print(f"{package} is not installed. Installing...")
        subprocess.check_call(['pip', 'install', package])

from cryptography.fernet import Fernet, InvalidToken
from PIL import Image
import smtplib
from email.mime.multipart import MIMEMultipart
from email.mime.image import MIMEImage
from email.mime.text import MIMEText
from email.mime.application import MIMEApplication
import re
```

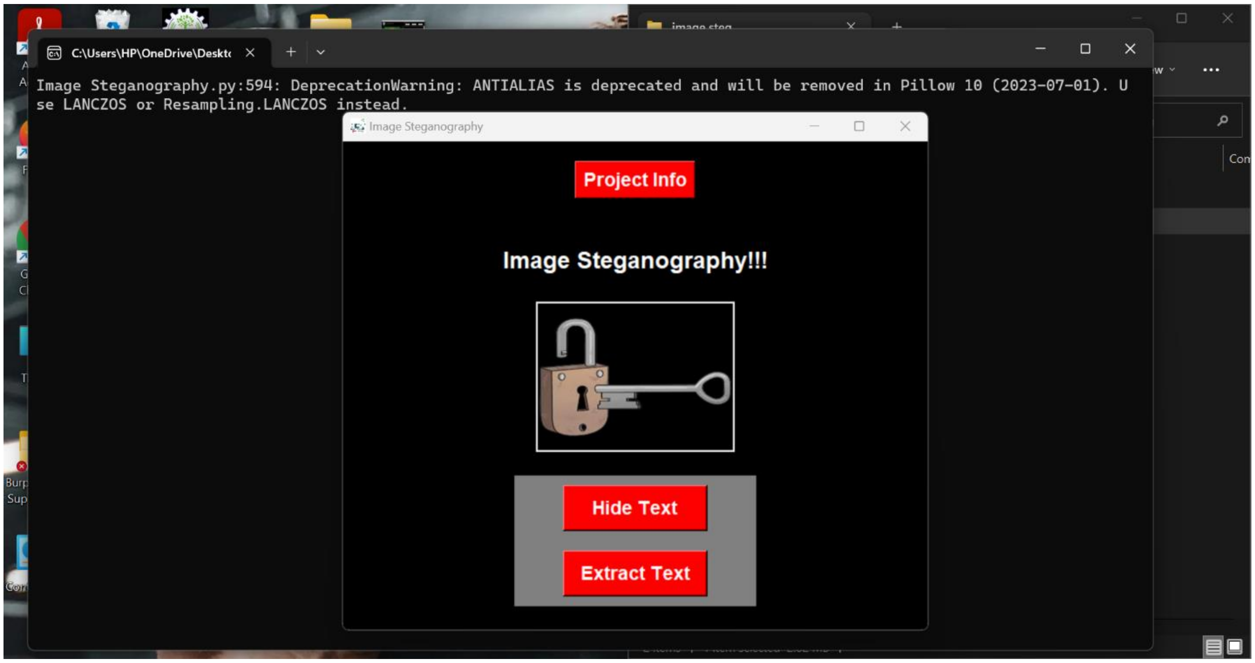
<u>Sending mail:</u> Sending mail for image steganography involves hiding a secret message or data within an image and then sending the steganographic image as an email attachment to the intended recipient. The recipient, who is aware of the steganography method used, can then extract the hidden message from the image to access the concealed information.



```
#Email details
sender_email = 'suprajatechnologiesprojects@gmail.com'
receiver_email = email
subject = 'The Key and Encrypted Image'
message = 'The Key for Encrypted Image is:\n'+str(key)

#Image details
image_path = output_path

#Create a multipart message
msg = MIMEMultipart()
msg['From'] = sender_email
msg['To'] = receiver_email
msg['Subject'] = subject

# Open the file in bynary
with open(image_path, "rb") as attachment:
    # Add file as application/octet-stream
    # Email client can usually download this automatically as attachment
    part = MIMEApplication(attachment.read(), Name=image_path)

# Add header
part["Content-Disposition"] = f"attachment; filename= {image_path}"

# Attach the file to the email
msg.attach(part)

#Add a text message to the email
msg.attach(MIMEText(message, 'plain'))

#SMTP server details
smtp_server = 'smtp.gmail.com'
smtp_port = 587
smtp_username = 'suprajatechnologiesprojects@gmail.com'
smtp_password = 'vadtydrxhhckkjef'

#Connect to the SMTP server
server = smtplib.SMTP(smtp_server, smtp_port)
server.starttls()
server.login(smtp_username, smtp_password)

#Send the email
try:
    server.send_message(msg)
except smtplib.SMTPRecipientsRefused:
    messagebox.showerror("Error", "Envalid Email Address")
    loading_window.destroy()
    return

#Disconnect from the email
server.quit()

# Close the loading window
loading_window.destroy()

# Show success message
messagebox.showinfo("Info", "Image encrypted successfully.")
```

Implementation of Hiding Text:

Step 1: Open the app then the below shown preview projects on to your screen. Click on **Hide Text.**



```
Image Steganography.py:594: DeprecationWarning: ANTIALIAS is deprecated and will be removed in Pillow 10 (2023-07-01). U
se LANCZOS or Resampling.LANCZOS instead.
```

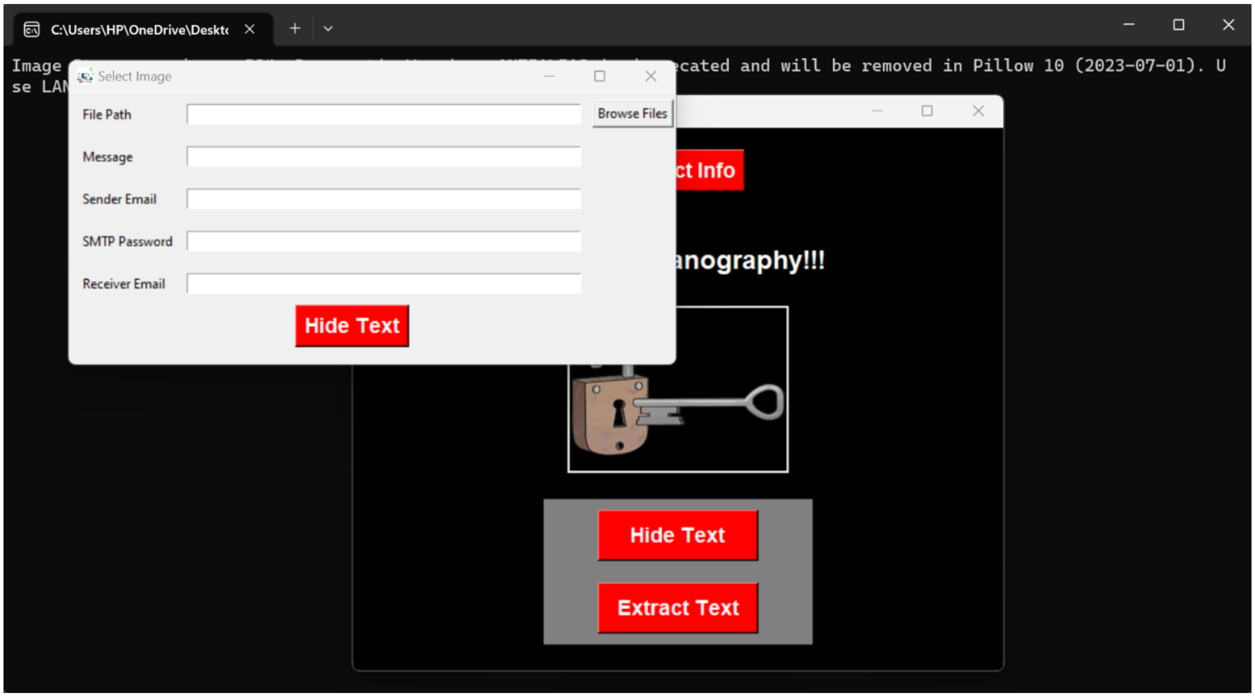
Step 2: After clicking on **Hide Text.** Another tab comes upon the preview. The shown boxes need to be filled by you for security purposes. Which is as follows:

File Path: Copy the file path and paste in the provided box, or else type the path of the file which you want to provide security.

Sender Email: This is the box in which the sender’s mail should be put in. The file you need to send will be sent through the mail you mention here.

SMTP Password (Simple Mail Transfer Protocol): The password is to be set by the sender which gives access to the receiver who wants to open the encrypted file.

Receiver Email: Mention the mail of person who the sender gives access to see it. Then click on hide text.



```
Image                                              ecated and will be removed in Pillow 10 (2023-07-01). U
se LAN
```

File Path

Message

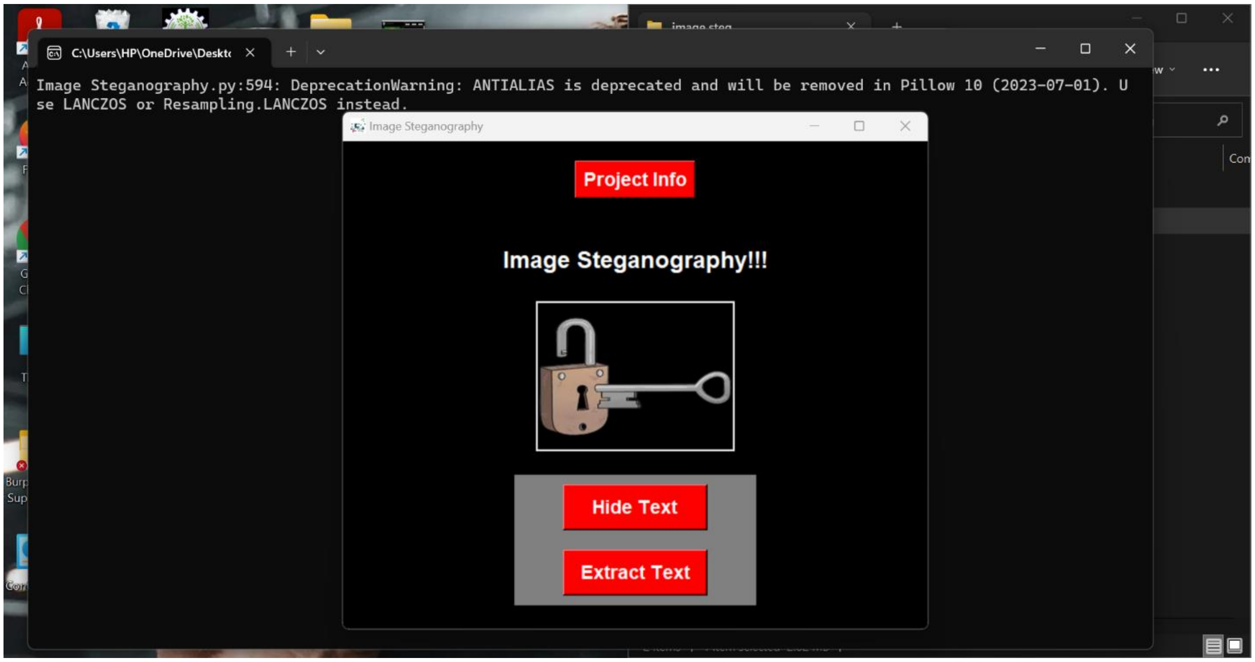
Sender Email

SMTP Password

Receiver Email

Implementation for Extract Text:

Step 1: Open the app then the below shown preview projects on to your screen. Click on **Extract Text**.

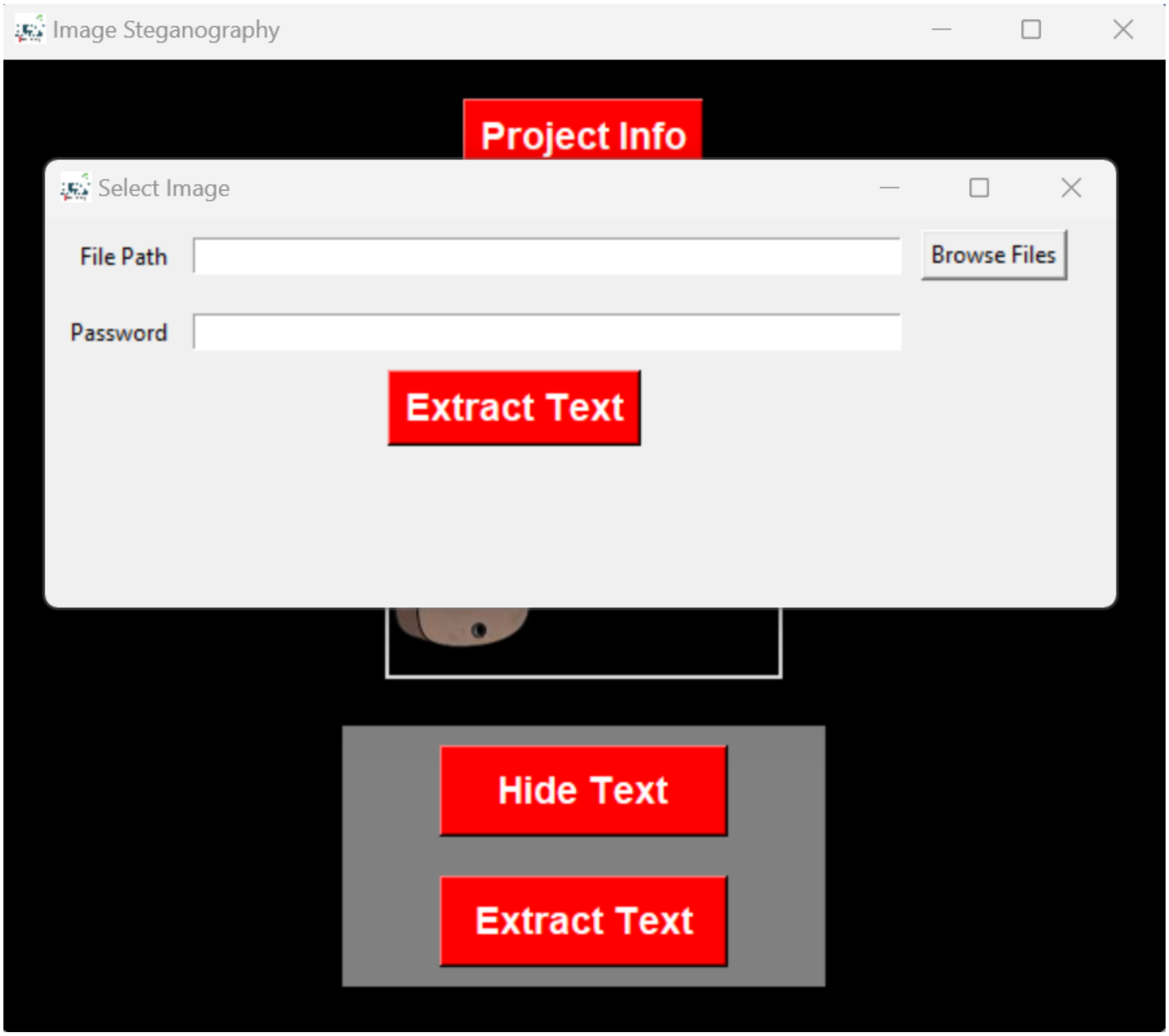


```
Image Steganography.py:594: DeprecationWarning: ANTIALIAS is deprecated and will be removed in Pillow 10 (2023-07-01). U
se LANCZOS or Resampling.LANCZOS instead.
```

Step 2: After clicking on **Extract Text.** The below picture appears on screen.

File Path: Put the file path which you want to extract the information from.

Password: Type the given password by the sender through sender's mail for accessing the hidden text.



Conclusion: The detailed description of Image steganography has been presented in this review. There exist various approaches for hiding secret information behind the cover image. Every detail regarding what type of image format is best suited and depending upon what type of requirement can decide that a particular steganographic algorithm is good or not. On the other hand, three different levels are used to tell the strength and weakness of a steganographic algorithm in particular parameter or requirement.

Different techniques to embed data inside the cover image have also been explained to the reader. The paper emerges with the idea to think about what types of factors should be kept in mind in order to come up with a new steganographic algorithm. The analysis shows that the transform domain techniques are best for the attack resilient system with relatively lower data capacity and higher complexity while the spatial domain is best for limited complexity systems and provides greater options for techniques selection for the systems with limited computational power.