iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52407

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Secret Communication Using Multi-Image Steganography with Face Recognition and OTP System

Prof. Sakshi Shejole[1], Priya Sawant[2], Rohini Jadhav[3], JyotiRajput[4], PratikshaNetke[5]
[1, 2, 3, 4, 5]*Department of Computer Engineering Alard College of Engineering, Pune Savitribai Phule Pune University*

Abstract: Our Proposed system is to develop a Web operation for hiding information in any image train to ensure the safety of the exchange of data between different military parties and give better security during communication transmission. We use the LSB fashion. The proposed approach uses a steganography algorithm to bed data in the image lines for military operations. For security purposes, we used modules face Recognition fashion with the AES algorithm for Strong Security purposes. And we use the cover channel fashion as an information-hiding fashion that can be exploited by a process to transfer information in a manner that violates the system security programs.

Image steganography is the main aspect of information caching where the ciphertext is bedded into an image called a cover image which is coming to insolvable for the interferers to see with their naked eyes. The retired information can be any textbook, images, audio, or indeed videos inside a cover image.

The abstract description ofMulti-image Steganography is that the secret law is divided into multiple corridors and is etched into multiple cover images. So we proposed two image steganography ideas to make it veritably grueling for the hackers to conceal the data. This paper proposes the Least significant bit(LSB) fashion of Steganography and the Advanced Encryption Standard(AES) fashion of Cryptography to make a safe and secure system. Then the sender and the receiver use the same key to encrypt and decipher the data which is popularly nominated a symmetric crucial Keywords AES Algorithm, LSB Algorithm, and Steganography.

I. INTRODUCTION

Designing a system for secret communication using multi-image steganography and face recognition The end of this design is to give security for data transferred over the network between two or further people. We use advanced technology, which is the OTP system in our design, to enhance the security position of information security. has come a high issue of worldwide concern. To ameliorate the validity and proficiency of the image data-caching approach, a slice-edge secret information concealment transmission scheme grounded on face recog- nition is proposed.

On the sender and receiver sides, we use the face recognition fashion for costing the sender and receiver secret dispatches, and the advanced technology we use is OTP technology. This technology can help to pass secret mes- pundits to the receiver without any hindrance. Generally, we use cryptography to encrypt in s sensitive dispatches in the form of textbooks. There are numerous algorithms professionally developed for sequestration.

AES(Advanced Encryption Standard)(10) is one of them listed. AES was an assiduity standard and surfaced as a largely effective jotting system due to the erected- advantage of better security with lower complex., there are remaining styles used to hide informa- operation gar¸con alone about to in any way that the mortal senses can descry. One similar fashion is steganography. Encryption is a popular and important algorithm that's extensively accepted n information security.

A. Cryptography

Cryptography can be defined as the process of guarding information and communication by using and integrating and interpreting translated dispatches, which can be demonstrated in situations where communication is estab- lished between two parties in an unsafe way that isn't fluently heard by third parties or outside the community. Cryptography contains a collection of encryption ways that include encryption and encryption fabrics, integrity, digital signing, data sequestration protection, and sequestration or communication services.

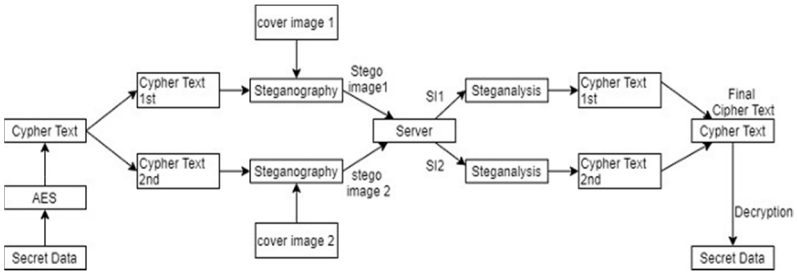


Figure 1: Proposed System

B. AES (Advanced Encryption Standard)

It was necessary to replace DES as its main size is veritably small. With the growth of computer power, it is considered a trouble to the full attack of hunt keys. DES triplets were designed to overcome this problem but were set up to be slow. This is where AES starts light, which is set up to be 6x times faster than TripleDES. The most popular and extensively accepted symmetric encryption algorithm that can be achieved momentarily is the Advanced Encryption Standard(AES). Unlike DES, in AES the number of cycles varies and depends on the length of the key. AES operates using '128-bit keys, 192-bit keys, and 256-bit keys ' with cycles of ' 10,12 and 14 ' independently. In ultramodern cryptography, AES is extensively accepted and supported on both tackle and software. To date, no effective cryptoanalytic attacks against AES have been detected. In addition, the AES has a fairly flexible crucial length, which allows for a position of ' unborn assurance ' against the development of the capability to perform critical quests. It has been 20 times since the launch of the AES but still nothing has been taken. current attacks, which is why it can safely be called the unbreakable standard of encryption. For these reasons, we will use AES in our proposed system approach.

It was necessary to replace DES as its main size is veritably small. With the growth of computer power, it is considered a trouble to the full attack of hunt keys. DES triplets were designed to overcome this problem but were set up to be slow. This is where AES starts light, which is set up to be 6x times faster than TripleDES. The most popular and extensively accepted symmetric encryption algorithm that can be achieved momentarily is the Advanced Encryption Standard(AES). Unlike DES, in AES the number of cycles varies and depends on the length of the key. AES operates using '128-bit keys, 192-bit keys, and 256-bit keys ' with cycles of ' 10,12 and 14 ' independently. In ultramodern cryptography, AES is extensively accepted and supported on both tackle and software. To date, no effective cryptoanalytic attacks against AES have been detected. In addition, the AES has a fairly flexible crucial length, which allows for a position of ' unborn assurance ' against the development of the capability to perform critical quests. It has been 20 times since the launch of the AES but still nothing has been taken. current attacks, which is why it can safely be called the unbreakable standard of encryption. For these reasons, we will use AES in our proposed system approach.

C. Steganography

In our design, we will be using the concept of steganography used to hide data. The word steganography is deduced from two Greek words ' steganos ' means the cover and ' plates ' means to write and generally refers to encryption or encryption. In this design, we use it to give security and sequestration. The content used to cipher the data is called the cover material, while the cover and the retired data are called the stego object.

D. Types of Steganography

Types of Steganography:

Image To Image Text To Image Image To Text Video To Voice Voice To Video

Our system uses textbook-to-image steganography. The simplest way to do this process is by fitting the nonpublic data bits in the LSB positions of digital images.

E. Text to image/ Image Steganography

Digital photography is a veritably safe way to manage sensitive information online using steganography. The picture is taken with the camera, the camera light will hear the commodity to be taken, and it'll be displayed on the camera screen. An image is a combination of pixels; image specification depends on the pixel. A pixel is a light nanosecond object on the display screen. The mortal eye can not descry pixels in an image.

Pixel is made up of three corridors. Three Red Pixels, Blue Pixel(R, G, and B). Each pixel has a depth of 24 by 3 bits. Each part is equal to one byte. Any color is made up of a combination of these three factors. The number of bytes varies from 0 to 255. The color will be displayed grounded on the number of bits, 0 is veritably dark and is veritably bright. The image size is given in pixels, for illustration, the image size is 600 * 450, and the image is a combination of pixels. The pixel is made up of three corridors on each part of an 8-bit size, for illustration, - pixel bits 0000000000000000 and the pixel will be red. Depending on the RGB values the pixel color will change. The translated communication that will be bedded within the image is converted into bits depending on its ASCII value. also, these pieces of data will be stored in the image depending on the steganographic process used. Steganography is associated with colorful advanced technologies where data is hidden in an image train. This can be done by changing the less important pieces in the original data.

F. Crypto-Steganography

With the help of LSB Steganography and the AES Algorithm fashion, we can apply high-position information security without covering image damage. Least Significant Bit(LSB) is a system in which the last part of each pixel is acclimated and replaced by data for private communication. The AES has a flexible erected-in within the main length, which allows for a position of" unborn assurance" against the progress of the capability to perform important crucial quests. For illustration, it's 128 bits long, that is, AES works on 128 bits of blank textbook to produce 128 bits of ciphertext.

G. OTP Sytsem

One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once, as the name suggests. The OTP feature prevents some forms of identity theft by making sure that a captured username/password pair cannot be used a second time.

Typically the user's login name stays the same, and the one-time password changes with each login.

One-time passwords (aka One-time passcodes) are a form of strong authentication, providing much better protection to eBanking, corporate networks, and other systems containing sensitive data. A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters that authenticates a user for a single transaction or login session. An OTP is more secure than a static password, especially a user-crCNN- based sword, which can be weak and/or reused across multiple accounts. OTPs may replace authentication login information or may be used in addition to it to add another layer of security.

II. RELATED WORK

The proposed model uses the AES cryptography algorithm and contains steganography styles an inheritable algorithm and a reconnection system. By using an inheritable algorithm it's possible to ameliorate the hunt in the perfect S to ameliorate the quality of the performing image. The reconnection process is integrated with an inheritable algorithm to induce new results by testing results. The author handed major changes to the circles that connect high-quality color steganography Advanced Encryption Standard(AES) to ameliorate security and ease of use with a focus on the Symmetric Key Cryptosystem and AES algorithm. This process focuses on hiding the image inside another large cover image. It also outlines a proposed way to ameliorate performance depending on both the secret communication volume and stego train quality. CNN- grounded styles are grounded on the depth of convolutional neural networks to bed and prize secret dispatches. the author proposes a system that uses both cryptography and steganography to insure two situations of data security. The purpose of this paper is to develop a new way to use XOR functionality for cracking data and embedding bedded images- aimlessly using a stoner-named key. To bed data within a cover image, The Steganography Bit(LSB) system has been used. The translated communication that will be bedded within the image is converted into bits depending on its ASCII value. likewise, in(6), the author introduced the stylish Least Significant Bit(LSB) system grounded on steganography image enhancement being LSB conversion ways to ameliorate the security position of translated information. I examine the colorful in-depth literacy styles set up in the image of steganography. In steganography, the cover image is used in such a way that the retired data isn't seen and therefore makes it less suspicious than in secret jotting. In discrepancy, Steganalysis is used to descry the presence of any secret communication covered in an image and to prize retired data.

III. PROPOSED SYSTEM

In our system, we use a system to hide data outside and the image is called print steganography. People can't make a difference or see when data is bedded in images. In our system, we use three- caste security videlicet. with login authentication, cryptography, and steganography give unrivaled high data security over the network.

In this system, the user gives secret data as input. After entering the secret data system will reckon the secret data and divide the cipher text into two corridors. After that two- cipher handbooks are bedded with cover images i.e. taken from the user apply dereliction images and produce stego images for separate cipher handbooks. also, shoot that image to the receiver. At the receiver end, the user will unite the stego images. after witnessing images decrypt the cipher text and combine the plain text. We get secret data and also display the secret data. In LSB Steganography, sheltered information is stored nearly in the LSB image Take the double representation of the sheltered information and overwrite the LSB of each byte within the cover image and make sure that you use a quality image to match that real face.

IV. METHODOLOGY

Steganography is the technique for hiding data and aims to hide data in such a way that any eavesdropper cannot observe any changes in the original media. Data hiding has two main branches, steganography, and watermarking. The present work focuses on steganography and uses images as the cover for 28 hiding secret data. Steganography conceals the secret data inside the cover image in such a way that no one can even know there is secret data there. Image steganography is common and used most widely in comparison to other types of steganography. This popularity is because images have a large amount of redundant data that can be used to hide secret data easily and because images take into consideration the advantage of the limited power of the human visual system (HVS). In image steganography, the original image is called the cover image, the stego image is the image that results from embedding secret data inside the original image. The cover and stego images should be more similar, so it will be harder for an unauthorized person to know the stego image. – Cryptography Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages.

It is evident in situations where two parties establish communication over an insecure medium. a medium that can be easily eavesdropped on. Cryptography is a pool of cryptographic techniques comprising encryption and decryption frameworks, integrity, check functions, and digital signature frameworks. Encryption frameworks alter secret messages into illegible formats for an unauthorized person. while decryption frameworks are used to decode the scrambled message by a person who has authorized to do so. The encryption aspect of cryptography is mainly for the protection of sensitive information and unsolicited alterations. It entails the encryption of stored data information as well as the encryption of the information to ensure secure communication. If an encrypted message is successfully intercepted by an eavesdropper, it will be useless to the attacker because an encrypted message cannot possibly be decrypted. by an authorized person. The value of the confidential data obtained from a system is the most essential factor. the thing to the attacker. The data may be compromised, distorted, or even deployed for future attacks by attackers. A perfect way of solving these problems would be to exploit the advantages of cryptographic and steganographic techniques to develop a hybrid system that can be stronger than the individual strengths of the component techniques.

V. EXPERIMENTAL RESULT

A system with a three-layer security will be developed to produce a very safe approach by merging image steganog- raphy with cryptography which will hide the text for secret communication. This system will be very difficult to hack, and nobody can detect secret communication between military personnel. This will provide an end-to-end encrypted communication system.

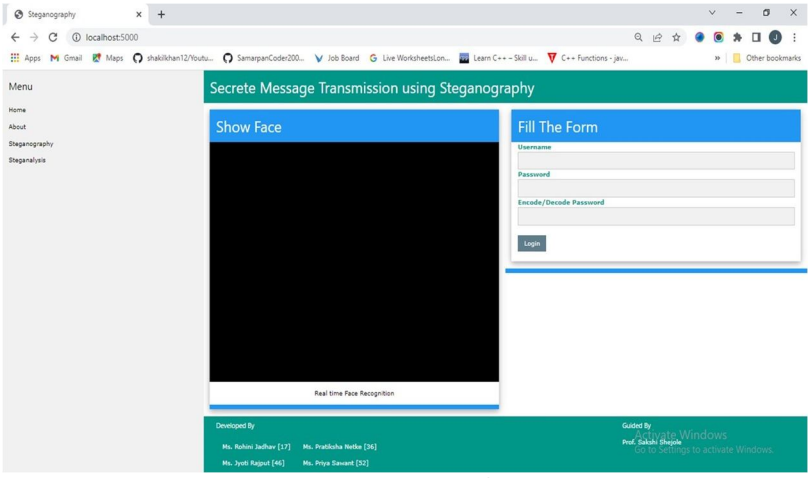


Figure 2: Login System

Following fig shows the login module of our system where the first security layer i.e. login authentication is established. in login page we get authenticate to the system via image recognition and getting OTP of particular authenticate user.

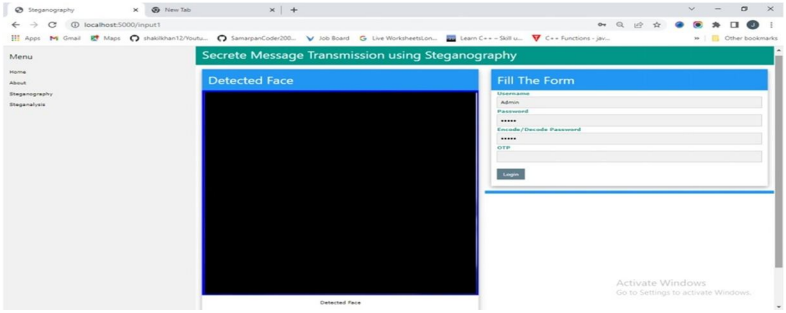


Figure 3: Login System

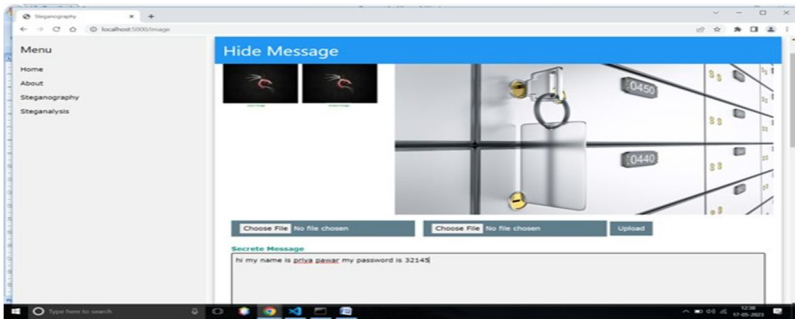


Figure 4: Encryption Interface

Figure 4 shows the stenography module which has the encryption interface where the user will select and upload two cover images as shown below to hide the secret text taken as input via the voice module into it post the encryption process. “This is a secret message” is the secret message we communicating here.

Figure 5 shows the receiver has to log in using the credentials and enter the same encode/decode password as that of the user whom he trying to communicate with. The steganalysis, a module is where the total decryption takes place. We retrieve the embedded ciphertext from the stego-images, merge them and then finally decipher it to get the original secret text as illustrated below. The proposed method is tested there; plain text (encryption) is first encrypted using the AES algorithm to produce ciphertext. The key is used based on the symmetric cryptosystem where the same key is used for the encryption process and the writing process. The ciphertext was then separated and embedded in two image files using the LSBbased steganography method. Then these stego images produced so much are sent to the intended recipient, where the retrieval process i.e. how to retrieve embedded messages from stego images and then the actual message is encrypted using the same key used during encryption. In this exercise we examine and compare the first image with a stego image obtained after using our proposed method and thus learn the percentage of change between the original image and the stego image.

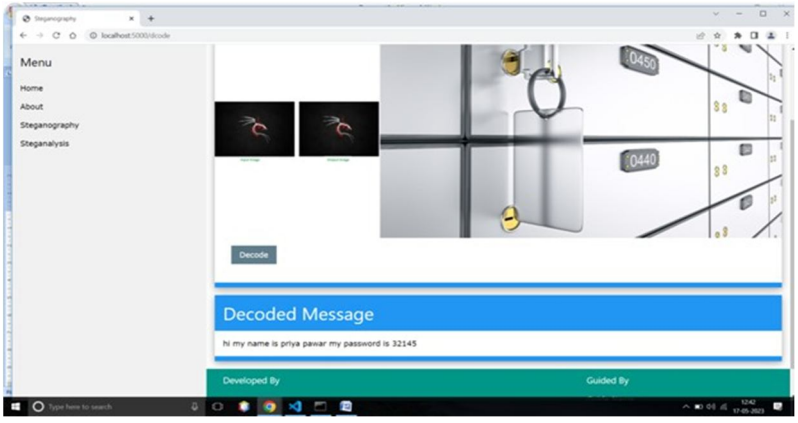


Figure 5: Decryption Interface

Designation	Value
Size of image in pixels	262144
Size of Image in Bits	26911456
Size of Message Encrypted in Bits	3264
Size of Message Encrypted and Compressed in Bits	4608
Percentage Of Compression	17%
Number Of bits Changed	3749
Percentage Changed	0.059%
Security Size	Security of AES key is 256 bits

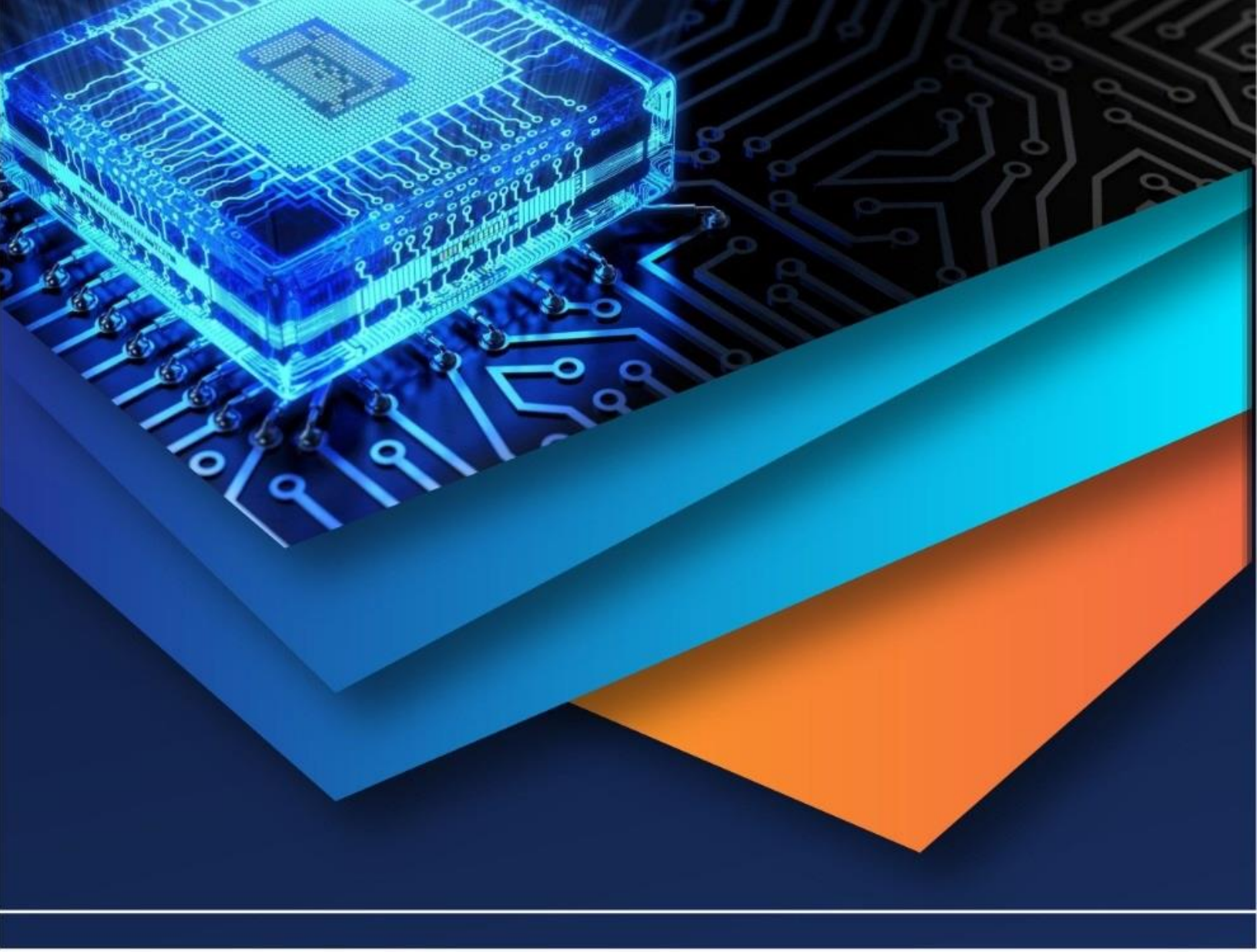
Figure 6: Figure: Result obtainted for proposed method

VI. CONCLUSION AND FUTURE WORK

In this project, we are designing a high level of information security without causing any damage to the cover image. using the LSB technique. When we are using the LSB algorithm, there will be fewer chances to lose data. It will be almost impossible for hackers to attack the stego image, as the cover and stego images look similar. In the future, we will be expanding our technique using a generative adversarial network (GAN). came into existence, which helps to generate networks without losing the properties of attributes such as the face. identity and orientation

REFERENCES

[1] Prateek Kumar Singh, Pratikshit Tripathi, Rohit Kumar, Deepak Kumar, IRJET, Secure Data Transmis- sion, Volume: 04 Issue: 04 — Apr-2017.
[2] Dalia Nashat* and Loay Mamdouh, An efficient steganographic technique for hiding data.
[3] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, Combination of Steganography and Cryptography: A short Survey, ICSET 2019
[4] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Ridrich, Ton Kalker," Digital Watermarking and Steganography"
[5] Hussein L. Hussein, Ahmed A. Abbass, Sinan A. Naji, Salam Al-augby and Jasim H. Lafta, Hiding text in a gray image using mapping technique, IOP Publishing 2018
[6] Deepesh Rawat and Vijaya Bhandari, Steganography technique for hiding text information in the color im- age using improved LSB method, IJCA 2013. Mehdi Hussain, A survey of image steganography techniques, IJAST 2013
[7] Hamad A. Al-Korbi, Ali Al-Ataby, Majid A. Al-Taee and Waleed Al- Nuaimy, Highly efficient image steganography using Haar DWT for hiding miscellaneous data, JJIT 2016
[8] Nitin Jirwan, Ajay Singh, Dr. Sandip Vijay, Review and analysis of cryptography techniques, IJSER 2013
[9] M. Karolin, Dr. T. Meyyappan, SM. Thamarai, Encryption, and decryption of color images using virtual cryptography, IJPAM 2018
[10] IJSTR VOL-8, ISSUE 12, DECEMBER 2019: Image Steganography Using LSB by Dr.Amarendra K Venkata Naresh Mandhala, B.Chetangupta, G.GeethaSudheshna, V.Venkata Anusha
[11] A.J. Raphael and V. Sundaram, "Cryptography and Steganography-A Survey", International Journal of Computer Technology and Applications, Vol. 2, No. 3, pp. 626-630, 2016
[12] K. Curran and K. Bailey, "An Evaluation of Image Based Steganography Methods," Multimedia Tools and Applications, Vol. 30 Issue 1, pp. 55 – 88, July 2006
[13] Image Steganography Using Steg with AES and LSB, - 2021 IEEE 7th International Conference on Com- puting Engineering and Design (ICCED)
[14] T. Jamil, "The rijndael algorithm," IEEE potentials, vol. 23, no. 2, pp. 36–38, 2004.
[15] SREELAKSHMI (2015, Nov 9), " Image Steganography using LSB,"https://www.slideshare.net/SreelekshmiSree1/image- steganography-using-lsb/
[16] IJEIT VOL-2, Issue 6, Dec 2012: Analysis and Comparison between AES and DES Cryptographic Algo- rithm. By Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma
[17] IJSRISSN(online): 2319-7064: A Comparative Study of Steganography and Cryptography by Pranali R. Ekatpure, Rutuja N Benkar.
[18] Aura Conci, Andre Luiz Brazil, Simone Bacellar Leal Ferreira, TruemanMacHenry, —AES Cryptography in Color Image Steganography by Genetic Algorithms
[19] Design and Implementation of a Modified AES Cryptography with Fast Key Generation Technique, —2020 IEEE International Women in Engineering Conference on Electrical and Computer Engineering(WIECONECE)
[20] An Improved Secret Message Capacity Using Modulus Function Based Color Image Data Hiding, —2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)
[21] Screenshots of checking plagiarism: (1)Abstract Plagarisum:



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY