IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 6, June 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

Secure Photo Sharing Social Networks Using Coverless Image Steganography Techniques

Mr.R.KARTHIKEYAN.,[1] Mr.R. MADHUBALA.,[2]

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal Tamilnadu, India[1]

PG Scholar, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamilnadu, India[2]

ABSTRACT: Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. Image steganography, aiming at using cover images to convey secret information has become one of the most challenge and important subjects in the field of information security recently. Different from the traditional image steganography, coverless image steganography does not need to employ the designated cover image for embedding the secret data but directly transfers secret information through its own properties such as pixel brightness value, color, texture, edge, contour and high-level semantics. Therefore, it radically resists the detection of steganalysis tools and significantly improves the security of the image. Its basic idea is to analyze the attributes of the image and map them to the secret information according to certain rules based on the characteristics of the attributes.This project proposes a digital image steganography framework without embedding data directly into the images that extracts the secret-data from the convolution neural network trained with the distance local binary pattern images from an indexed image database.

KEYWORDS: Steganographic Encoder function; Social Networking Services (SNS); Redundant Pattern Encoding; Grayscale images.

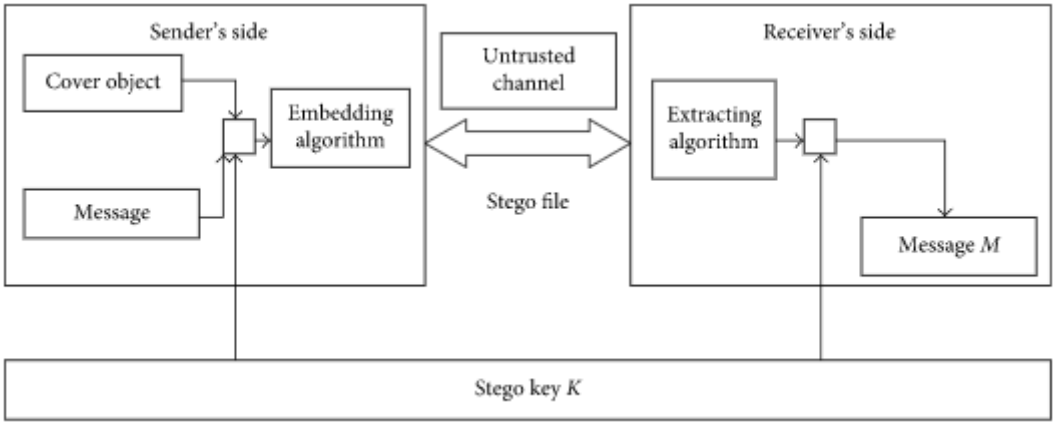
I. INTRODUCTION

With today's ubiquitous internet service, digital images can be conveniently downloaded and shared through social networking services (SNS) such as Facebook, Snapchat, Twitter, etc. Therefore, there are vital needs to provide some mechanisms to manage – originally was 'protection' the vast number of originals images. Information hiding (i.e., data embedding) is the process of inserting external information (e.g., ownership information and secret message) into a medium. It is one of the possible solutions to serve the aforementioned needs. Fig. 1 illustrates the general framework during the data embedding process. Data is inserted into the cover image with a secret key to produce an output image with embedded data, while aiming to achieve high perceptual image quality, large embedding capacity, and strong resistance to attacks.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

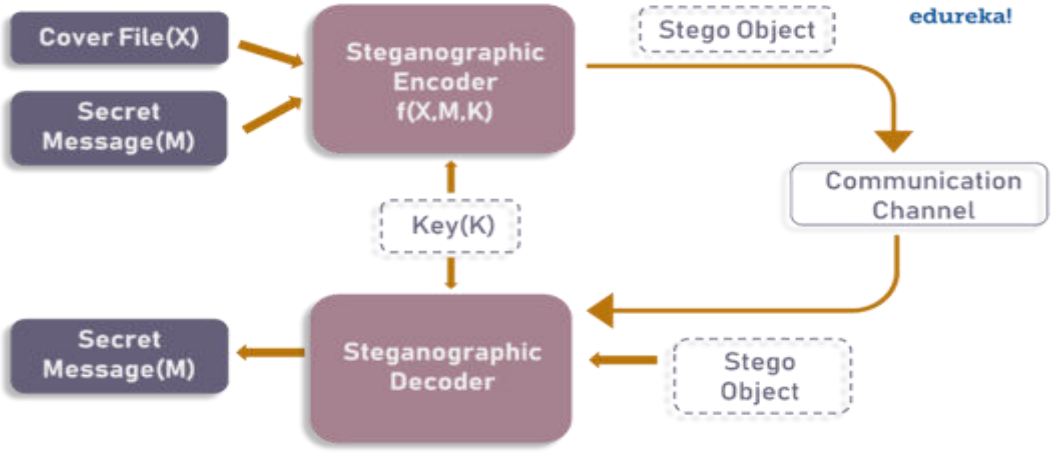
|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |



In the image domain, the application of information hiding can be coarsely categorized as watermarking and steganography. Watermarking is the practice of visibly or invisibly embedding information into images to render the ownership. It can be retrieved for the purposes of claiming ownership during a dispute or to detect tampering of content for integrity checking purpose. On the other hand, steganography is the art and science of concealing the existence of the secret communication via a cover such as image, video, audio, text, etc. The embedded information should be unnoticeable, or in specific, perceptually undetectable by humans.

Steganography is the art and science of embedding secret messages in a cover message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message The diagram below depicts a basic steganographic model.



As the image depicts, both cover file(X) and secret message(M) are fed into steganographic encoder as input. Steganographic Encoder function, f(X,M,K) embeds the secret message into a cover file. Resulting Steno Object looks very similar to your cover file, with no visible changes. This completes encoding. To retrieve the secret message, Stego Object is fed into Steganographic Decoder.

II. LITERATURE SURVEY

Authors in [1] proposed robustness and capability of resisting image steganalysis, a novel coverless image steganography algorithm based on discrete cosine transform and latent dirichlet allocation (LDA) topic classification is proposed. In this paper [3], latent dirichlet allocation topic model is

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

utilized for classifying the image database. Second, the images belonging to one topic are selected, and 8 × 8 block discrete cosine transform is performed to these images. Then robust feature sequence is generated through the relation between direct current coefficients in the adjacent blocks. In this paper [5], an inverted index which contains the feature sequence, dc, location coordinates, and image path is created. For the purpose of achieving image steganography, the secret information is converted into a binary sequence and partitioned into segments, and the image whose feature sequence equals to the secret information segments is chosen as the cover image according to the index. After that, all cover images are sent to the receiver. In the whole process, no modification is done to the original images.

III. STEGANOGRAPHY TECHNIQUES

Depending on the nature of the cover object (actual object in which secret data is embedded), steganography can be divided into five types:

- Text Steganography
- Image Steganography
- Video Steganography
- Audio Steganography
- Network Steganography

Text Steganography - Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

- Format Based Method
- Random and Statistical Generation
- Linguistic Method

Image Steganography - Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image. Common approaches include:

- Least Significant Bit Insertion
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Coding and Cosine Transformation

Audio Steganography - In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to others, such as Image Steganography. Different methods of audio steganography include:

- Least Significant Bit Encoding
- Parity Encoding
- Phase Coding

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

- Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

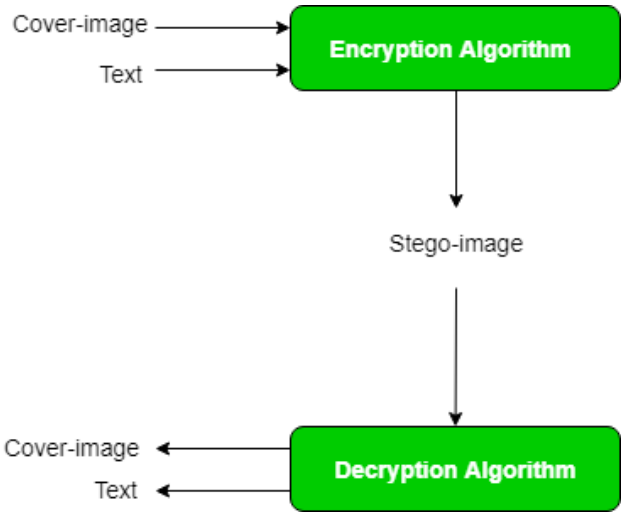
Video Steganography - In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

- Embedding data in uncompressed raw video and compressing it later
- Embedding data directly into the compressed data stream

Network Steganography (Protocol Steganography) - It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

Image Steganography - As the name suggests, Image Steganography refers to the process of hiding data within an image file. The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image.

An image is represented as an N*M (in case of greyscale images) or N*M*3 (in case of colour images) matrix in memory, with each entry representing the intensity value of a pixel. In image steganography, a message is embedded into an image by altering the values of some pixels, which are chosen by an encryption algorithm. The recipient of the image must be aware of the same algorithm in order to known which pixels he or she must select to extract the message.



Detection of the message within the cover-image is done by the process of steganalysis. This can be done through comparison with the cover image, histogram plotting, or by noise detection. While efforts are being invested in developing new algorithms with a greater degree of immunity against such attacks, efforts are also being devoted towards improving existing algorithms for steganalysis, to detect exchange of secret information between terrorists or criminal elements.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

IV. PROPOSED SYSTEM

Since the concept of coverless information hiding was proposed, it has been greatly developed due to its effectiveness of resisting the steganographic tools. Most existing coverless image steganography (CIS) methods achieve excellent robustness under non-geometric attacks. However, they do not perform well under some geometric attacks. Towards this goal, a CIS algorithm based on DenseNet feature mapping is proposed. Deep learning is introduced to extract high-dimensional CNN features which are mapped into hash sequences. For the sender, a binary tree hash index is built to accelerate index speed of searching hidden information and DenseNet hash sequence, and then, all matched images are sent. For the receiver, the secret information can be recovered successfully by calculating the DenseNet hash sequence of the cover image.

- We propose a novel hash mapping rules based on CNN feature, and it improves the robustness against geometric attacks. Compared with other manual features, it is more able to capture the global features of the image when losing some content. Besides, we also do a series of experiments on existing network model and chose the optimal network model (DenseNet).
- An efficient binary tree hash index based on bitwise indexing is designed to speed up the search of cover images for secret information.

The framework of the proposed approach is composed of three parts, which are implemented in four steps: generation of hash sequence, construction of binary tree hash index, coverless image steganography, and extraction of secret information. In our approach, the pre trained Dense Net model is firstly used to extract the features of the image database.

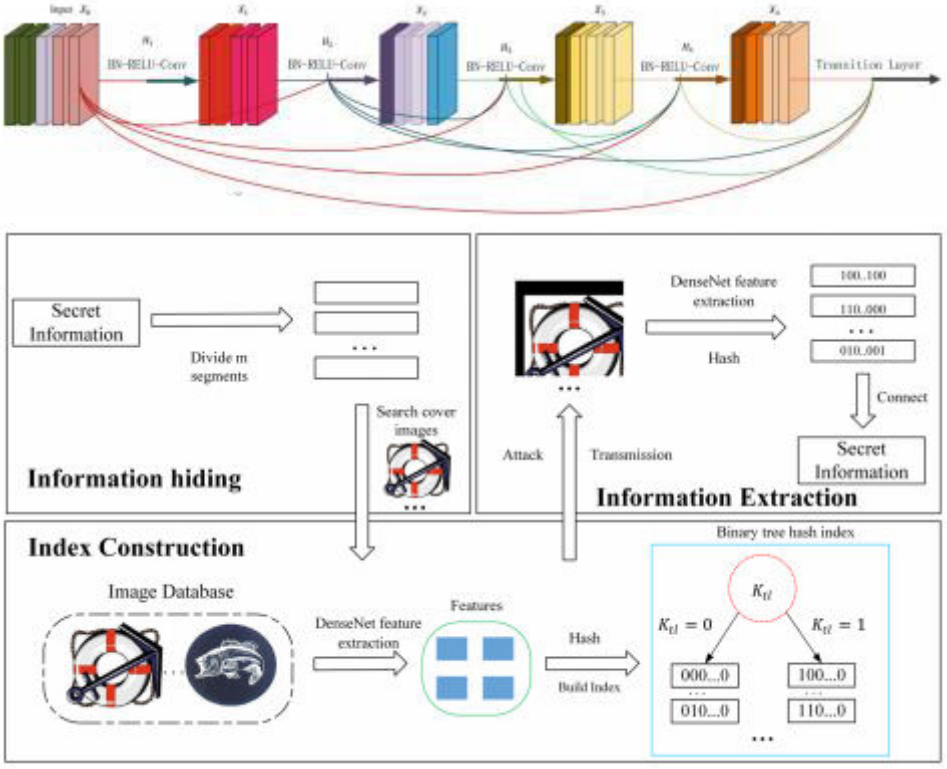


Fig 4.1 hash algorithm

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

block is calculated. Then, feature coefficients Me are scanned by "arithmetic scan"(steplength set to sl) to generate the hash sequence. Next, the secret information is divided into segments equal to the hash sequence N, and the search cover images are searched through matching with the hash sequence. Finally, all cover images sent to the receiver in order, such that the receiver could recover secret information by calculating received images under the same hash algorithm. Considering that the length of the sequence may not be a multiple of N, 0 is filled in the last segment of the partition, and the number of 0 is recorded in the last image.

V. SYSTEM OVERVIEW - MODEL IMPLEMENTATION

- **SN Web App -** Build a social networking service is an online platform in which people use to build social networks or social relationships with other people who share similar personal or career interests, activities, backgrounds or real-life connections. Social networking services vary in format and the number of features.
- **Register -** Users in this application, who want to access and share their images into this site, they should register their information in this site. After they registered their data in this site, they can log into the application for providing and accessing images which are shared by their friends or some other persons in social networks. Users can not only look at the images from this site, but also, they can upload their images either by private or public. In which, users can give friend requests, accept friend requests, and key request to reveal private images in the site.
- **Login -** The user will demonstrate social network features wherein he will perform following operations: [1] Edit Profile [2] View and Add Friends [3] Search Users [4] View User Profile
- **Add Friends /Family Groups -** Friend Request A log in/out button could be used for log in/out with the social website. After logging in, a greeting message and the profile picture will be shown. This prototype works in three modes: a setup mode, a sleeping mode and a working mode.
- Picking Close Friends, A user needs to manually specify the set of "close friends" from their friend list on social website and form the neighbourhood by clicking the button "Pick friends".
- **Share/Post/Comment/Chat -** Sharing Photo User can share a photo only to friends on list. According to the proposed scheme, this friend list should be intersection of owner's privacy policy and co-owners' exposure policies. Policy mining: Users can establish the uploaded image whether the image is private or public; then eligible users (friend only view the public images) can access these images otherwise images will be hidden. If users want to view private content, then the content owner should provide the key for that image. Policy mining is carried out within the same category because images in the same category are more likely under a similar level of privacy protection. E) Policy prediction: In this phase they generate several candidate policies while the goal of this system is to return the most promising one to the user. Thus, it presents an approach to choose the best candidate policy that follows the user's privacy tendency. It provides a predicted policy of a newly uploaded image to the user for their reference

Request/Response - To respond to a friend request, you have two choices. One is to click one of the two buttons to the right of your potential friend's name. One button reads Confirm and one

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

reads Not Now. Click one of those buttons and (respectively) you add a friend or ignore the request quietly.

Photo Privacy:-

➢ **Key Generation -** In this process, privacy information of the photo is protected by using the selected protection tool and a secret key (or a set of keys) set by the sender. Apart from providing a proper security level and an efficient implementation, one relevant challenge is to properly manage all the encryption keys used in the system. We propose a centralised approach where all keys are stored in the trusted Key Server.It is essential that the server is able to uniquely identify images in order to be able to generate unique keys for each picture and region in it. As we have mentioned, the Key Server randomly generates a unique identifier for each protected picture that is sent back to the LockPic application at encryption time. This unique ID is included in the metadata of the encrypted picture. Another approach could be to use the hash of the picture as ID. The problem of using the hash as the ID is that the hash has to be performed in the mobile application, which might be an expensive operation depending on the size of the picture, and could present security problems in the case that hash collisions are found. More importantly, the key server would be able to analyse some usage patterns as it would be able to recognize if two different users encrypt the same picture.

Photo and Message Encode/Decode:-

➢ **Image and Message Encoding -** Our encoder network consists of down sampling layers, residual layers, and up sampling layers. In the resent, it includes many skip connections to fuse the shallow features and deep features in the different convolution stages. The shallow feature includes a lot of low-level efficient information about the outline and color of image, which is very beneficial for the generation of steganographic images.

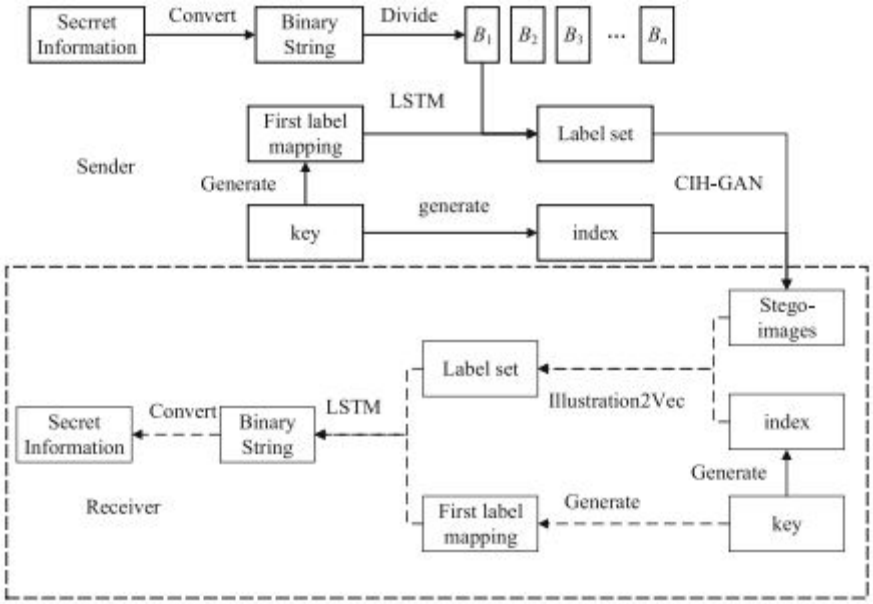


Fig 5.1 Generation of Steganographic Images

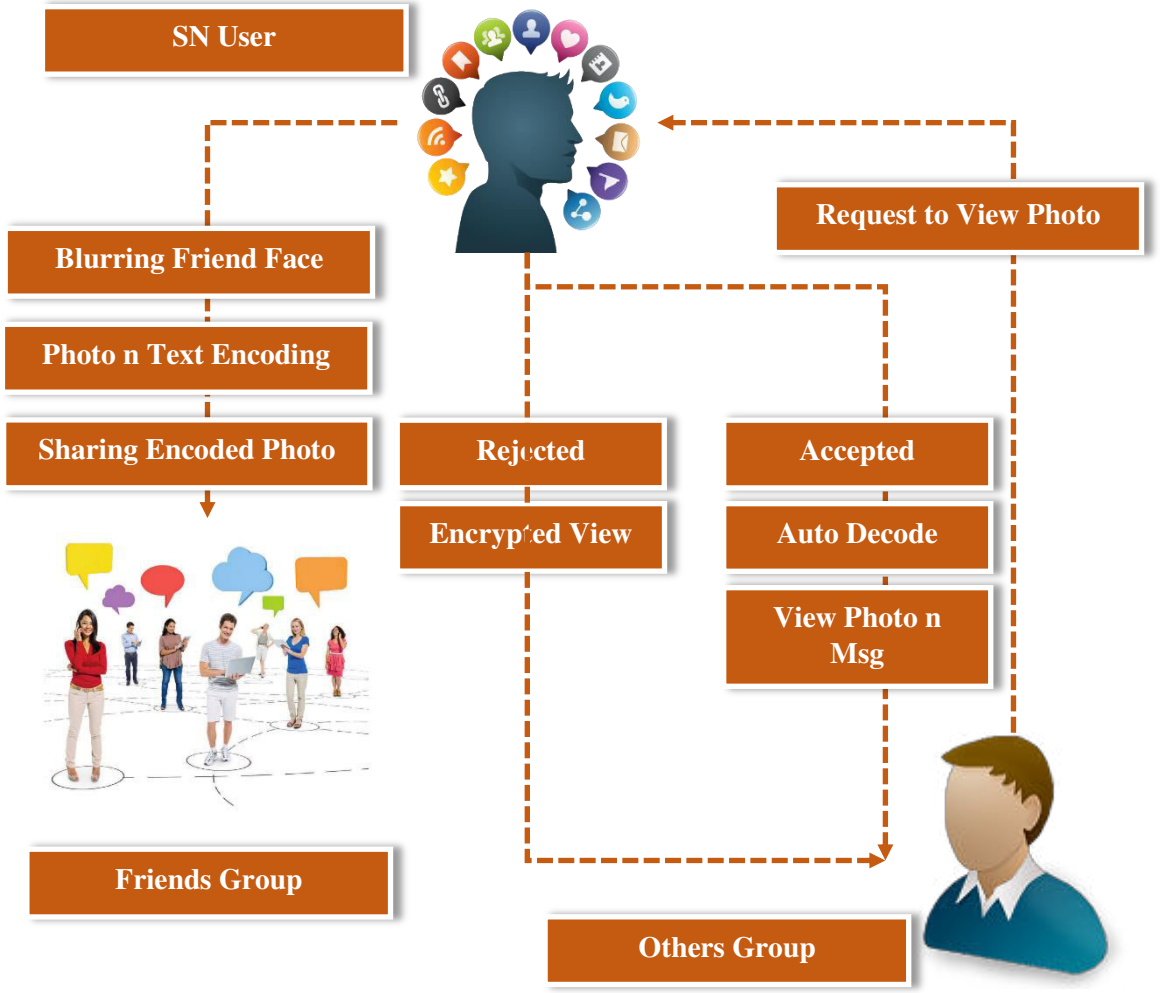
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

a. original image b. generated image

VI. SYSTEM DESIGN



VII. FUTURE ENHANCEMENT

The next plan is to develop a steganography technique that is robust to different types of attacks and also work can be enhanced for other data files like audio, video, and text. By these methods we can achieve best completeness, correctness, quality and accuracy.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

VIII. CONCLUSION

This paper proposed a new idea for CIH. Driven by secret information and constrained by attribute labels, it directly generates anime character with high quality to transmit secret information. Compared with the current cover selection methods, proposed method has a great improvement in capacity. However, there is a gap in robustness compared with the current robust coverless information hiding methods. The next step is to improve the robustness of the method by optimizing the generation model. This paper provides a more practical solution for the development of coverless information hiding, that is, to express secret information in the process of generating target images according to attributes, which has certain guiding significance for the development of coverless information hiding.

REFERENCES

1. R.Karthikeyan, & et all ”Biometric for Mobile Security” in the international journal of Engineering Science & Computing, Volume7,Issue6, June 2017, ISSN(0):2361-3361,PP No.:13552-13555.
2. R.Karthikeyan, & et all ”Data Mining on Parallel Database Systems” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:13922-13927.
3. R.Karthikeyan, & et all ”Ant Colony System for Graph Coloring Problem” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14120-14125.
4. R.Karthikeyan, & et all ”Classification of Peer –To- Peer Architectures and Applications” in the international journal of Engineering Science & Computing, Volume7,Issue8, Aug 2017, ISSN(0):2361-3361,PP No.:14394-14397.
5. R.Karthikeyan, & et all ”Mobile Banking Services” in the international journal of Engineering Science & Computing, Volume7,Issue7, July 2017, ISSN(0):2361-3361,PP No.:14357-14361.
6. R.Karthikeyan, & et all ”Neural Networks for Shortest Path Computation and Routing in Computer Networks” in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:86-91.
7. R.Karthikeyan, & et all ”An Sight into Virtual Techniques Private Networks & IP Tunneling” in the international journal of Engineering and Techniques, Volume 3 Issue 4, Aug 2017, ISSN:2395-1303,PP No.:129-133.
8. R.Karthikeyan, & et all “Routing Approaches in Mobile Ad-hoc Networks” in the International Journal of Research in Engineering Technology, Volume 2 Issue 5, Aug 2017, ISSN:2455-1341, Pg No.:1-7.
9. R.Karthikeyan, & et all “Big data Analytics Using Support Vector Machine Algorithm” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 6 Issue 9, Aug 2018, ISSN:2320 - 9798, Pg No.:7589 -7594.
10. R.Karthikeyan, & et all “Data Security of Network Communication Using Distributed Firewall in WSN ” in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 6 Issue 7, July 2018, ISSN:2320 - 9798, Pg No.:6733 - 6737.
11. R.Karthikeyan, & et all “An Internet of Things Using Automation Detection with Wireless Sensor Network” in the International Journal of Innovative Research in Computer and

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2023 ||

| DOI:10.15680/IJIRSET.2023.1206125 |

Communication Engineering, Volume 6 Issue 9, September 2018, ISSN:2320 - 9798, Pg No.:7595 - 7599.

12. R.Karthikeyan, & et all "Entrepreneurship and Modernization Mechanism in Internet of Things" in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, Pg No.:887 - 892.
13. R.Karthikeyan & et all "Efficient Methodology and Applications of Dynamic Heterogeneous Grid Computing" in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, Pg No.:1125 - 1128.
14. R.Karthikeyan & et all"Entrepreneurship and Modernization Mechanism in Internet of Things" in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, Pg No.:887– 892.
15. R.Karthikeyan & etall"Efficient Methodology for Emerging and Trending of Big Data Based Applications" in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 7 Issue 2, Feb 2019, ISSN:2320 - 9798, Pg No.:1246– 1249.
16. R.Karthikeyan & et all "Importance of Green Computing In Digital World" in the International Journal of Innovative Research in Computer and Communication Engineering, Volume 8 Issue 2, Feb 2020, ISSN:2320 - 9798, Pg No.:14 – 19.
17. R.Karthikeyan & et all "Fifth Generation Wireless Technology" in the International Journal of Engineering and Technology, Volume 6 Issue 2, Feb 2020, ISSN:2395–1303.
18. R.Karthikeyan & et all "Incorporation of Edge Computing through Cloud Computing Technology" in the International Research l Journal of Engineering and Technology, Volume 7 Issue 9, Sep 2020 ,p. ISSN:2395–0056, e. ISSN:2395–0072.
19. R.Karthikeyan & et all "Zigbee Based Technology Appliance In Wireless Network" in the International Journal of Advance Research and Innovative Ideas in Education, e.ISSN:2395 - 4396, Volume:6 Issue: 5 , Sep. 2020. Pg.No: 453 – 458, Paper Id:12695.
20. R.Karthikeyan & et all "Automatic Electric Metering System Using GSM" in the International Journal of Innovative Research in Management, Engineering and Technology, ISSN: 2456 - 0448, Volume:6 Issue: 3 , Mar. 2021. Pg.No: 07 – 13.
21. R.Karthikeyan & et all "Enhanced the Digital Divide Sensors on 5D Digitization" in the International Journal of Innovative Research in Computer and Communication Engineering, e-ISSN: 2320 – 9801, p-ISSN: 2320 - 9798, Volume:9 Issue: 4 , Apr. 2021. Pg.No: 1976 – 1981.
22. R.Karthikeyan & et all "Crop Yield Prediction Based On Indian Agriculture Using Machine Learning" in the International Journal Of Engineering and Techniques, ISSN: 2395-1303, Volume:8 Issue: 4 , July. 2022. Pg.No: 11 – 22.
23. R.Karthikeyan & et all "A Blockchain Approach to Ensuring Provenance to Outsourced Cloud Data in A Sharing Ecosystem" in the International Journal Of Multidisciplinary Research In Science, Engineering and Technology, ISSN: 2584-7219, Volume: 5 Issue: 7, July. 2022. Pg.No: 1740 – 1744.
24. R.Karthikeyan & et all "College Bus Transport Management Web Application" in the International Journal Of Multidisciplinary Research In Science, Engineering and Technology, ISSN: 2582-7219, Volume: 6 Issue: 6, June. 2023. Pg.No: 1619 – 1625.
25. R.Karthikeyan & et all "Face Recognition Based Attendance System" in the International Journal of Innovative Research in Computer and Communication Engineering, ISSN: e 2320-9801, Volume: 11 Issue: 6, June. 2023. Pg.No: 8710 – 8717.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details