IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SMART IMAGE STEGANOGRAPHY USING SECRET KEY

[1]Prof.Pragati Mahale, [2]Mr.Hrushikesh Kale, [3]Ms.Meera Keshattiwar, [4]Mr.Mrunal Patil, [4]Ms.Aakanksha Shinde

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
Department of Information Technology,
AISSM'S Institute of Information Technology,
Pune-1, Maharashtra, India

Abstract: Steganography is used to conceal information such as text, photos, and videos in other media files such as photographs, videos, and music. We can use steganography to safely transport communications from one host to another. Currently, we cannot rely on the server side to encrypt our communications from beginning to finish because the server side knows both the sender and receiver's keys. We can ensure that the server does not decode and keep our messages in plain text by using steganography. We can protect our messages both from the server and from outsiders. With steganography, we save our secret data in the pixels' least significant bits. Putting data in the least significant bits haslittle effect on the picture since the pixel values fluctuate significantly. We may encrypt data into graphics using several strategies such as sequential, prime, and equation ciphering. To interpret such a picture, the intruder must search for all possible combinations of pixels, which raises the task's temporal complexity exponentially. We may usethis strategy to secure our communications not just from attackers but also from server-side proxy attacks. With thisapproach, the transmitter and receiver agree on some keys that will be used to encrypt and decrypt data from photographs. Only two keys must be remembered by the user: the beginning point and the method used to encrypt data into the Pictures.

Index Terms **- Data Hiding, Steganography, Cyber Security, Cryptography, Data Security, Secure Communication.**

I. INTRODUCTION

Secret messages may now be communicated by disguising them in a photo or text so that only the sender and recipientcan read or see them. Steganography is the process of hiding and disclosing data. The image that covers the data in steganography is known as the cover image because it conceals the hidden message. The picture is known as the stego- image once the data has been buried. LSB insertion is a popular and widely used steganography technique for embedding data in a cover file[1]. The LSB embedding technique conceals data in the LSBs of the cover file, such that even the human eye cannot discover the hidden information. It is a strategy in the spatial domain[1]. Steganography is a method of disguising text in images such that if an intruder discovers the secret message, the intruder cannot read it. As a result, employing steganography will provide an additional layer of security. Picture compression is used to reduce the size of a message, allowing it to be easily buried. Image compression is an important application in Digital Image Processing. We can protect our messages both from the server and from outsiders. Withsteganography, we save our secret data in the pixels' least significant bits. Putting data in the least significant bits haslittle effect on the picture since the pixel values fluctuate significantly. We may encrypt data into graphics using several strategies such as sequential, prime, and equation ciphering. This is one of the most secure methods of sharing sensitive information.

II. EXISTING SYSTEM

Most contemporary systems simply employ steganography to obscure data, not to transfer it between two parties. Also, existing messaging apps can access messages on the server side, which is impossible to prohibit. Messaging apps such as Telegram and Facebook Messenger may observe conversations between two users and use this information to display tailored adverts. In many circumstances, data is not leaked to the outside world, but when it does, millions of users' data are exposed, which might be exploited for immoral reasons. In today's environment, datais crucial but also expensive. Intruders can sell this information for a high price. We don't want to rely on server-sideprograms to secure our data to avoid this from happening. A user cannot rely on an application to secure its data whilestill profiting from it. Data breaches are both unexpected and costly. The present data transmission options do not provide a method in which a user may totally own the keys used to encrypt and decode data.

III. PROPOSED SYSTEM

The program will be used to transport messages via steganography, which will strengthen the application's security. Because the invader is unaware of any message ciphered into the picture. This makes it more secure than cryptographyon its own. We may improve security even further by leveraging information known only to the sender and receiver.We will develop a web application for encrypted communications that will employ both encryption and steganography. Messages will be ciphered on the sender's client and decrypted on the receiver's side. This does not rely on the server since data is ciphered and decrypted at the client rather than the server. To ensure safe transmissionof sensitive information using pictures and the steganography technique: There are times when we cannot rely on third-party software to encrypt our messages while transferring confidential information to another user. In these cases, we can hide our encrypted data in media files. This prevents hackers from detecting the actual data being transmittedacross the network, even if it has been exposed. To decipher the data ciphered into media files, a key that identifies the right algorithm to encrypt and decrypt data from the file will be utilized.

IV. METHODOLOGY

The two clients can begin conversing with one another by exchanging private keys. With the key, the clients will be able to decode the incoming messages. To send the private key, a client encodes it into an image using a preset location and ciphering procedure. The other client can decode messages using the known location and scheme by extracting the private key from the image. As a result, our method employs steganography to carry out a key exchange. The method for encoding data into images is based on modifying the bits of a pixel. Each pixel's alpha, red, green, and blue bytes carry at least two significant bits, totaling one byte of information. One big disadvantage of modifying onlythe data-containing pixels is that there will almost certainly be variations in the neighboring pixels, which may makepicture analysis easier. Because to this weakness, a user's private key might be made public, potentially leading to message interception. To avoid this problem, we will additionally adjust the random and neighboring pixels in photosto make steganalysis more difficult. To decode a picture, a client must know the position of the initial pixel as well asthe ciphering algorithm used to encrypt the data. Individuals can transmit this information through voice messages, hints, or other physical mediums. The advantage of using this technique versus exchanging long, complex keys is that there is less, easier information to know

The two clients can begin conversing with one another by exchanging private keys. With the key, the clients will be able to decode the incoming messages. To send the private key, a client encodes it into an image using a preset location and ciphering procedure. The other client can decode messages using the known location and scheme by extracting the private key from the image. As a result, our method employs steganography to carry out a key exchange. The method for encoding data into images is based on modifying the bits of a pixel. Each pixel's alpha, red, green, and blue bytes carry at least two significant bits, totaling one byte of information. One big disadvantage of modifying onlythe data-containing pixels is that there will almost certainly be variations in the neighboring pixels, which may makepicture analysis easier. Because to this weakness, a user's private key might be made public, potentially leading to message interception. To avoid this problem, we will additionally adjust the random and neighboring pixels in photosto make steganalysis more difficult. To decode a picture, a client must know the position of the initial pixel as well asthe ciphering algorithm used to encrypt the data. Individuals can transmit this information through voice messages, hints, or other physical mediums. The advantage of using this technique versus exchanging long, complex keys is that there is less, easier information to know.

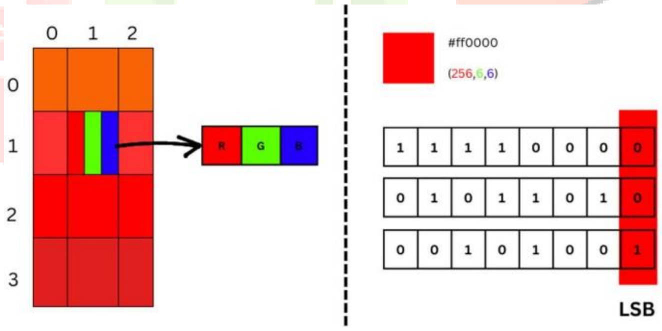


Figure 1. Pixel Representation

Bitwise operators such as &, — and ! are used to change the bits of a pixel. As a consequence, the bits in the requiredplace can be altered to correspond to the bit in the data. We can make this process easier by creating a stream of bits from the secret data, which we can then use to decide which bit in the cover image has to be changed next. We keepthe secret data in a queue-like data structure, so this process has some cost. Also, huge files lengthen the time requiredto distort a picture before encrypting it. Strong security is offered, but computational power is sacrificed. The picturein the preceding image contains a total of w*h pixels, where w is the width of the image and h is its height. We maytry to decode the image using the information from the n-queens problem with a little adjustment to the n-queens answer. Because this is not a chase, we may select any of the remaining pixels to be the next data point.

V. WHY QUANTUM RESISTANT ?

A quantum computer finds a private key associated with a public key by trying all the possible combinations of private keys. Symmetric key cryptography with large key size is resistant to quantum computers as there is no key which is made public. Using steganography, we are hiding a key into a large data by sharing a very small key which is easy toremember and share. As there is no direct involvement of public key and also to brute force all combinations of keysfrom host data to much time is required.

VI. ALGORITHMS USED

Data Cipher: To encrypt data into visuals, the least significant bit algorithm is utilised. Data is turned into a queue of bits in this procedure, which are subsequently placed into the image at the appropriate locations. The order of the bits where data is ciphered is determined by the location of the pixel and the method used. The user previously transmitted these two items using a verbal channel.

Camouflage Data: When we modify the pixels in an image, there is a risk that someone may notice a change in the adjacent pixels. With this information, the key may be extracted from the picture. To get around this problem, we make random changes to image pixels so that the read change blends in with other changes.

Data Decipher: The information included in the least significant bits is decoded using the first pixel's position and the scheme. The data are stored in a certain order depending on the ciphering scheme used. A 16-bit number is appended to the beginning of the data to indicate its length. In the first stage, we convert the first 16 bits of the pictureto integers. The length of the content, as seen in the image, is this. After extracting the content length, we begin to extract the true information from the data. The ciphering algorithm used dictates where the bits and pixels are arranged.

Key Exchange Algorithm: To exchange keys, two clients utilize a key exchange method based on steganography. Auser generates a public key and a private key, after which the public key is sent to another user. One user encrypts data using the public key of another user, who then gets the encrypted data. Another option for speeding up communication is symmetric key cryptography. Yet, asymmetric key cryptography is more secure than symmetric key cryptography.

VII. SYSTEM ARCHITECTURE.

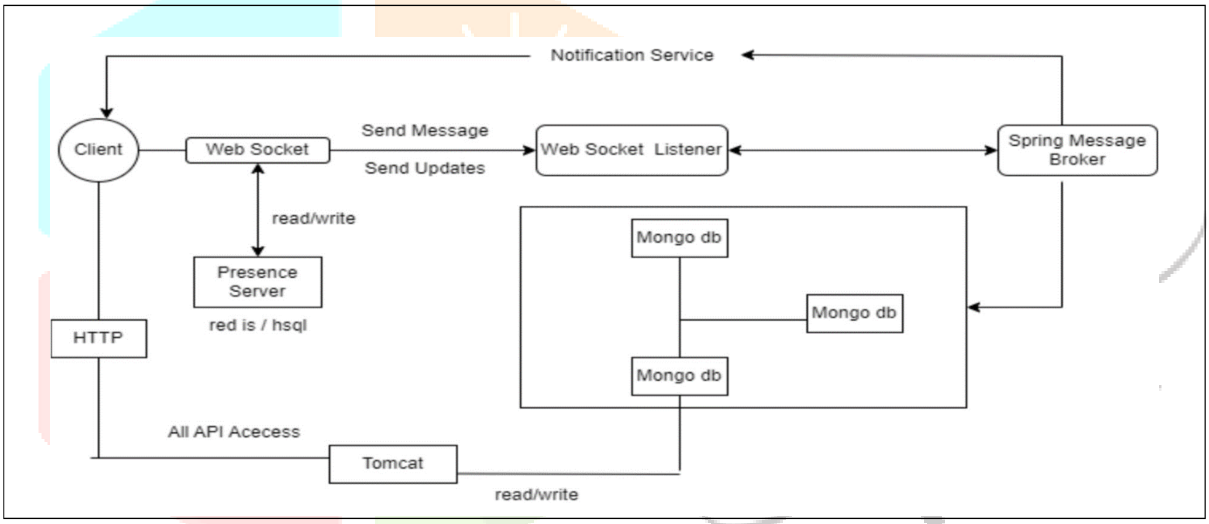


Figure 2. System Architectuture.

The methods of secret text encoding as a picture and secret data extraction from the image are shown in the above figure. It includes the cover image, the confidential information, and the key needed to encrypt and decrypt the data from the image. An summary of the procedure for encrypting data into images can be obtained by looking at the steganography process' architectural design. First, we need a background image that will hide information. The effectiveness of the algorithm depends on the size of the cover image used. If the image is large, there will be many possible interpretations, making the decoding procedure extremely challenging and time-consuming. The image must be sent to the other end over a channel, which may or may not be private, after data has been cloaked in it. Since thedata is hidden inside the cover image, the message is unaffected by the channel's security and it is not obvious to attackers whether a message is being sent or not. To decrypt a picture, the user must be aware of the initial pixel fromwhich the ciphering process started as well as the method used to encode the data into the image. The attacker is allowed to experiment with different combinations of the message's decoding tools and sites. This step must be completed either manually or with the support of a deep learning neural network in order to understand what the textsignifies. However, there are an infinite number of possible combinations of locations and techniques, making it practically impossible to complete this job. The number of possible permutations is 823543 for a picture with a breadth and height of 7 pixel. In reality, though, we might use images that are much bigger. The number of deciphering possibilities is approximately 1, with 30000 zeroes following that, if we use a picture with dimensions of 100 by 100.As was previously stated, the algorithm's strength is significantly influenced by the size of the image; as image size grows, algorithm strength rises exponentially.

VIII. RESULT ANALYSIS.

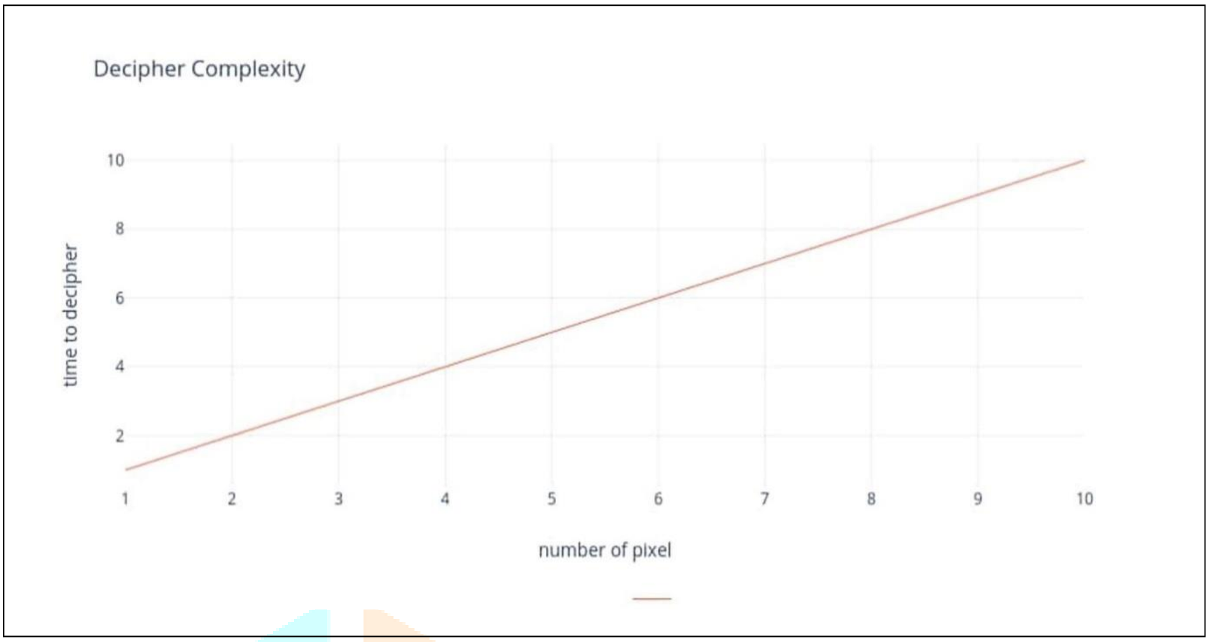


Figure 3. Decipher Complexity of Existing System.

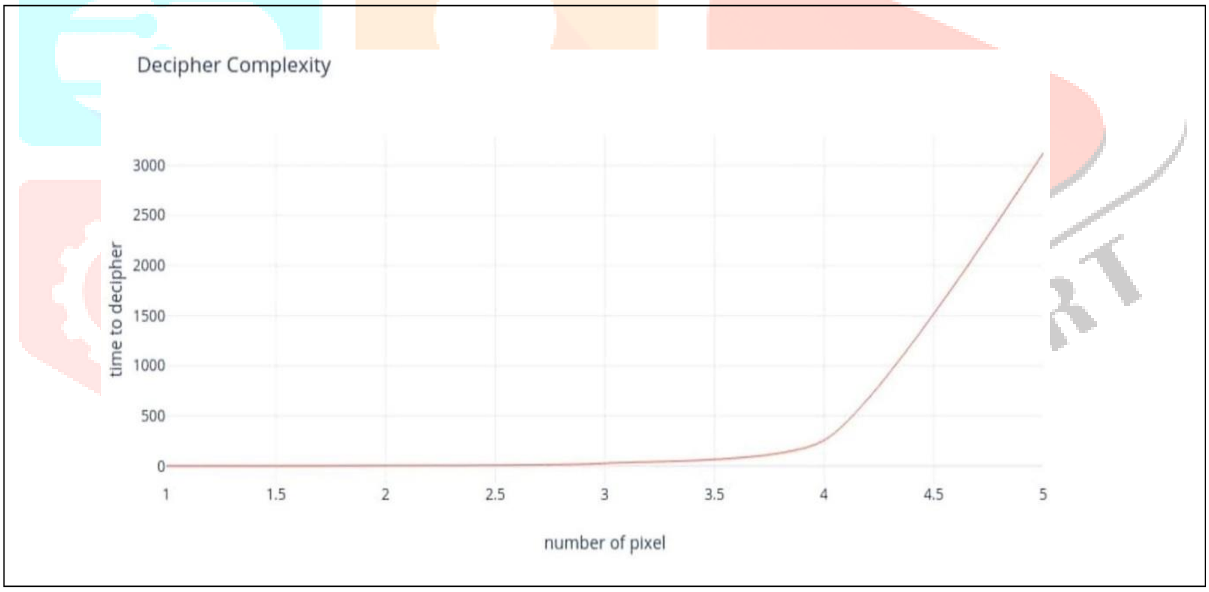
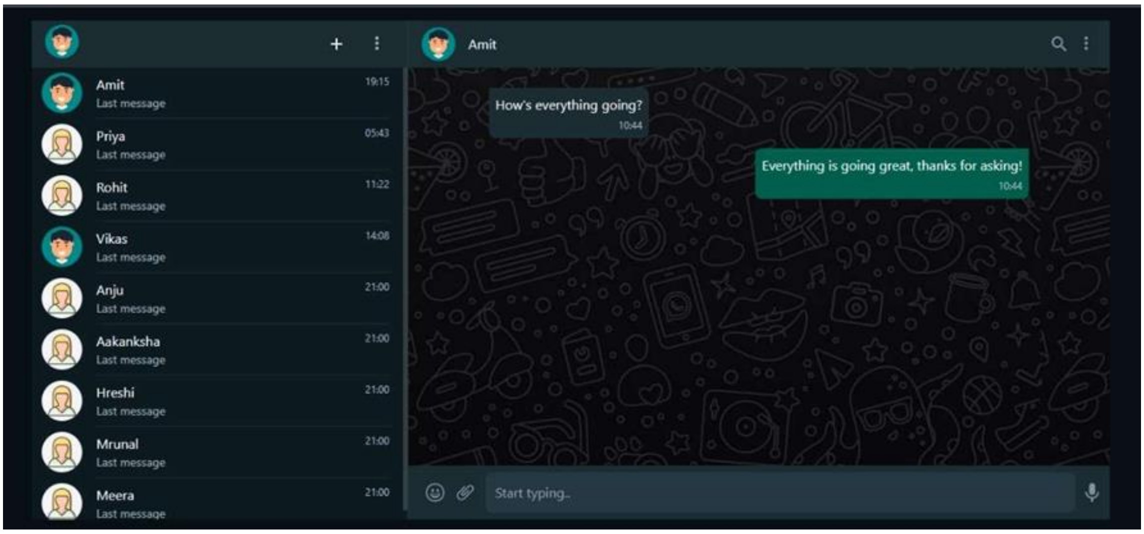


Figure 4.Decipher Complexity of Proposed System.

IX. OUTPUT



How's everything going?
10:44

Everything is going great, thanks for asking!
10:44

Figure 5. Chat Window

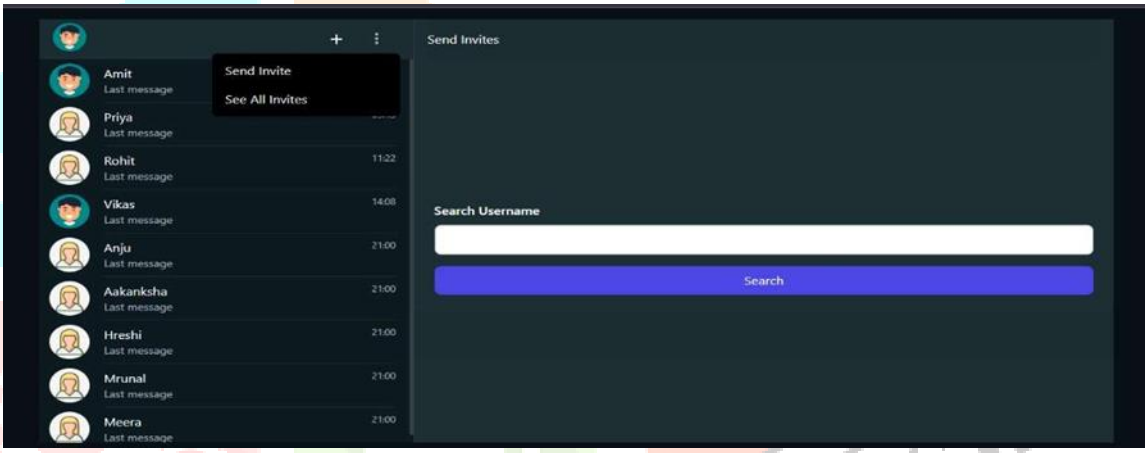


Figure 6. Send Invitation

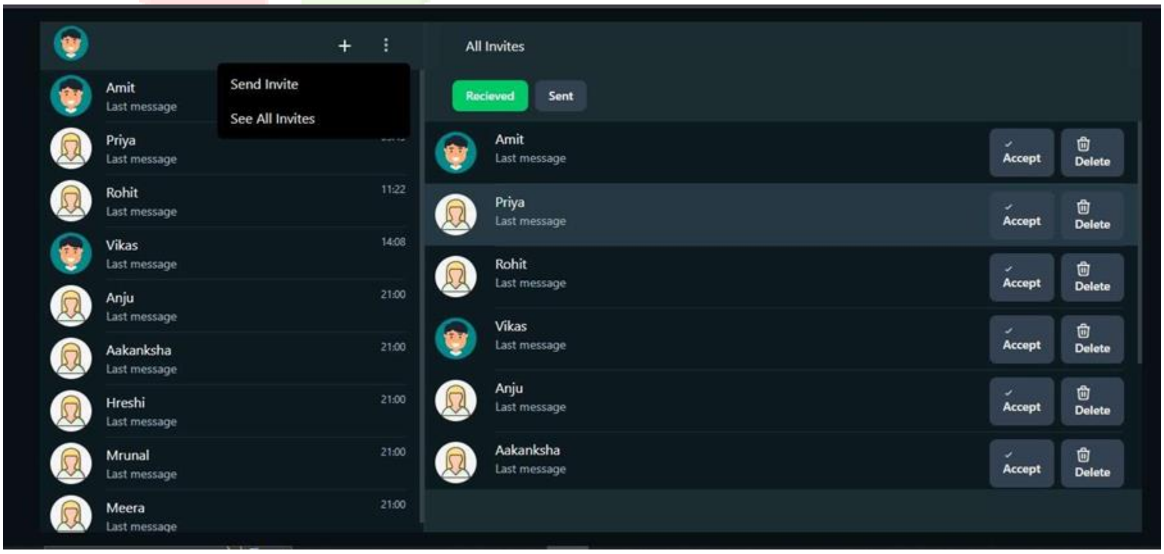


Figure 7. Receive Invitation

X. CONCLUSION

For the purpose of preserving the uniqueness of data, steganography can be implemented in many different contexts.The use of steganography in encrypted communication programs, where the keys are transmitted using Steganography, is one method. We may transmit data secretly from server side decryptions as well as external intruders by using our suggested paradigm for data exchange. In the majority of messaging apps, using decryption keys, messages can be easily decrypted on the server side. Any intruder or attacker will have to verify all the key combination combinations from the image using the method we have suggested. The process of extracting the keys from the picture is exponentially time-consuming. Additionally, while decoding the picture, the attacker must manually or using a sophisticated algorithm determine whether or not his/her decode is successful. Such an operationhas a high time complexity. We may exchange vast amounts of data from one customer to another with very little information from the clients. If the picture size is n*m, the time required for decoding is proportional to the number of pixels in the image.

XI. REFERENCES

[1] Osama Fouad Abdel Wahab, Ashraf A. M. Khalaf, Aziza I. Hussein, Hesham F. A. Hamed, “Hiding Data Using Efficient Combination of RSA Cryptography and Compression Steganography Techniques”, IEEE, Issue:2021.

[2] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, Ahmed Bouridane , “Image Steganography: A Review of the Recent Advances” , IEEE , Issue:2021.

[3] Asha Durafe, Rutika Desai, “Steganography for Public Security” , IEEE , Issue:2020.

[4] Ali Salem Ali, Mohammed Sabbih Hamoud Al-Tamimi, Alaa Ahmed Abbood, “Secure Image Steganography Through Multilevel Security”, International Journal of Innovation , Creativity and Change, IJICC , Issue:2020.

[5] manshu Arora, Cheshta Bansal, Sunny Dagar,”Comparative study of image steganography techniques” , International Conference on Advances in Computing, Communication Control and Networking, Issue : 2018

[6] Ammad Ul Islam1 , Faiza Khalid2 , Mohsin Shah2 , Zakir Khan2 , Toqeer Mahmood3 , Adnan Khan2 , Usman Ali2 , Muhammad Naeem4 , “An Improved Image Steganography Technique based on MSB using Bit Differencing” , The Sixth International conference on Innovative computing technology,Issue : 2016

[7] Ravi K Sheth,Rashmi M. Tank , “Image Steganography Technique”, Academia , Issue:2015

[8] Manveer Kaur , Gagandeep Kaur, “Review of Various Steganalysis Techniques”, IJCSIT, Issue:2014

[9] Abdalbasit Mohammed, Nurhayat Varol,”A Review Paper on Cryptography ”, Research Gate , Issue: 2019