# Novel Data Hiding in Images with Noise Filtration and Integrity Validation

[1] Jyoti Gupta,[2]Sandeep Toshniwal
[1]M.Tech Research Scholar ,[2]Associate Professor
[1,2] Department of Electronics & Communication Engineering,Kautliya Institute of Technology & Engineering, Jaipur, Rajasthan, India.

***Abstract :*** Data Security with authenticity and integrity of the data or information is the main problem and almost all the user deals with this issue. This paper presents the secure communication model with the noise and integrity constraints handling using SHA and MD5 for the integrity validation and the Median filter concept of the noise resolution in the communication of the data. This paper presents the steganographic way of sending the text in images with the integrity and noise filtration**.**

***IndexTerms*** **– Image Steanography , Noise Filteration ,Median Filter ,SHA, MD5.**

## I. INTRODUCTION

Steganography incorporates an immense range of methods for concealing messages in an assortment of media. Among these strategies are undetectable inks, microdots, computerized marks, undercover channels and spread-range correspondences. Today, on account of present day innovation, steganography is utilized on content, images, sound, sign, and that's just the beginning. The upside of steganography is that it tends to be utilized to covertly transmit messages without the reality of the transmission being found. Regularly, utilizing encryption may distinguish the sender or collector as someone with something to stow away. For instance, that image of your feline could hide the designs for your organization's most recent specialized development.

Nonetheless, steganography has various impediments too. In contrast to encryption, it for the most part requires a ton of overhead to shroud a moderately couple of bits of data. Be that as it may, there are ways around this. Likewise, once a steganographic framework is found, it is rendered futile. This issue, as well, can be survived if the concealed information relies upon a type of key for its inclusion and extraction. Truth be told, it is basic practice to encode the concealed message before setting. it in the spread message. [1].

.

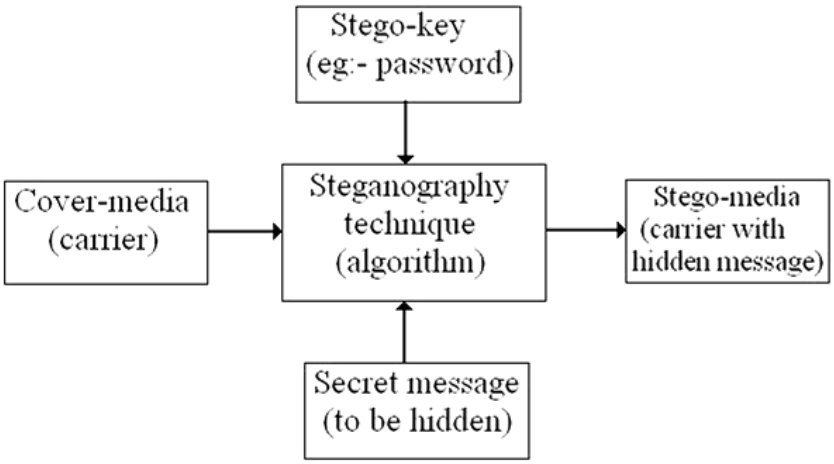


Fig1.1 Block diagram of steganography

The data to be covered up in the spread information is known as the "installed" information. The "stego" information is the information containing both the spread sign and the "implanted" data. Legitimately, the preparing of putting the covered up or implanted information, into the spread information, is now and then known as inserting. Sometimes, particularly when alluding to image steganography, the spread image is known as the holder.

In the accompanying three segments we will attempt to demonstrate how steganography can and is being utilized through the media of content, images, and sound. Frequently, despite the fact that it isn't essential, the concealed messages will be scrambled. This meets a necessity presented by the "Kerckhoff guideline" in cryptography. This rule states thatthe security of the framework must be founded on the suspicion that the foe has full information of the plan and usage subtleties of the steganographic framework. The main missing data for the adversary is a short, effectively replaceable irregular number arrangement, the mystery key. Without this mystery key, the adversary ought not get the opportunity to try and speculate that on a watched correspondence channel, shrouded correspondence is occurring. The greater part of the product that we will examine later meets this rule. [2]

When inserting information, it is essential to recollect the accompanying limitations and highlights: The spread information ought not be fundamentally debased by the implanted information, and the installed information should be as vague as could reasonably be expected. (This does not mean the inserted information should be undetectable; it is workable for the information to be covered up while it stays on display.) The implanted information ought to be legitimately encoded into the media, as opposed to into a header or wrapper, to keep up information consistency crosswise over format.[3]

## II. CRYPTOGRAPHY

It is a study of composing which changes over plaintext into figure content. During the time spent cryptography, it will scramble the whole message with the goal that it can't be comprehended by the outsider. In Cryptography, a key is connected to create scrambled content and to unscramble the encoded content. The contribution of cryptography procedure is a plain-content and the yield will be figure content. There are two sorts of cryptographic key: symmetric key and deviated key. In the symmetric key calculation, utilizes same key for encryption or unscrambling. It is likewise called as private key. In the deviated key calculation diverse keys are utilized for encryption and decoding. It is additionally called as open key.[4]

| Algorithm | Key size | Block size | Rounds | Status |
|---|---|---|---|---|
| DES | 56- Bits | 64-Bits | 16 | Cracked |
| RC2 | 128- Bits | 64- Bits | 16 mix 2 mashing | Cracked |
| RC4 | Variable | Variable | Unknown | Cracked |
| Blowfish | 128- Bits | 64-Bits | 16 | Not Cracked Yet |
| Towfish | (128, 192, 256)-Bits | 128- Bits | 16 | Not Cracked Yet |
| 3-DES | (112, 168)- Bits | 64-Bits | 48 | Not Cracked Yet |
| AES(Rijndael) | (128, 192, 256)-Bits | 128- Bits | 10, 12, or 14 | Not Cracked Yet |

Fig 2 .Popular Encryption Algorithms

## III. IMAGE FILTERING

The Purpose of smoothing is to lessen noise and improve the visual nature of the image. An assortment of calculations for example straight and nonlinear-calculations are utilized for sifting the images. Image sifting makes conceivable a few helpful undertakings in image handling. A channel can be connected to decrease the measure of undesirable noise in a specific image as appeared in fig. Another sort of channel can be utilized to turn around the impacts of obscuring on a specific picture. Nonlinear channels have very unique conduct contrasted with direct channels. For nonlinear channels, the channel yield or reaction of the channel does not comply with the standards laid out before, especially scaling and move invariance. Also, a nonlinear channel can create results that change in a non-natural manner.[5]

Defected image Real image

Fig 3 A Defected image and real image after applying filtering

### 3.1 Median filtering

In signal handling, it is regularly alluring to have the option to play out some sort of noise decrease on an image or sign. The middle channel is a nonlinear computerized separating procedure, frequently used to evacuate noise. Such noise decrease is a run of the mill preprocessing venture to improve the consequences of later preparing (for instance, edge on an image). Middle sifting is all around broadly utilized in computerized image preparing on the grounds that, under specific conditions, it jelly edges of the images while evacuating noisee.[10].

## IV. SHA ALGORITHM

Group of SHA contain four SHA calculations; SHA-0, SHA-1, SHA-2, and SHA-3. Despite the fact that from same family, there are basically unique.

- The unique form is SHA-0, a 160-piece hash work, was distributed by the National Institute of Standards and Technology (NIST) in 1993. It had couple of shortcomings and did not turn out to be prominent. Later in 1995, SHA-1 was intended to address asserted shortcomings of SHA-0.
- SHA-1 is the most broadly utilized of the current SHA hash capacities. It is utilized in a few generally utilized applications and conventions including Secure Socket Layer (SSL) security.
- In 2005, a technique was found for revealing impacts for SHA-1 inside commonsense time span making long haul employability of SHA-1 dicey.
- SHA-2 family has four further SHA variations, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash esteem. No effective assaults have yet been accounted for on SHA-2 hash capacity.
- Though SHA-2 is a solid hash work. In spite of the fact that essentially extraordinary, its fundamental plan is as yet following structure of SHA-1. Consequently, NIST called for new aggressive hash capacity structures.
- In October 2012, the NIST picked the Keccak calculation as the new SHA-3 standard. Keccak offers numerous advantages, for example, proficient execution and great opposition for attacks.[5]

## V. LITERATURE SURVEY

Mohit Sharma et al [6] in this paper have conceived the idea where they can move the image or content starting with one client then onto the next. For the situation they can first login as sender where creators can send the message which must be content or an image containing the concealed text.Then they can likewise login as a beneficiary which can get to the messages send to that person, where the instant messages are seen legitimately and the images contained the shrouded content require to be decoded by the client.

Inspiration: From this paper creators have enlivened in regards to the idea of the image steganography, that is concealing the content in the images just as the creator likewise presented the one of a kind idea of the protected document move of the images.

Aman Arora et al [7]Advancement of innovation and quick Internet made data to go over the world in a simple and conservative manner. This has made individuals to anguish about their protection. Steganography is a method that impedes unapproved clients to approach the significant information. There are different steganographic techniques that clients can use to stow away and blend data inside other data that make it challenging to perceive by unapproved clients. This paper gives a diagram of LSB procedure of steganography and further creators proposed and actualized a one of a kind calculation to base steganography which is an upgraded and improved strategy better in all angles. The paper further contrasts our proposed upgraded method and the current LSB strategy on different parameters to demonstrate viable and tasteful outcomes.

Inspiration: From this creator has altered our elements of the inserting and removing the content in the images and sound utilizing the idea of the LSB.

S. Sugathan [8] Steganography is one of the well known strategies in data concealing that enables individuals to impart furtively. The fundamental preferred position of image steganography is that the image inside which the mystery is encoded does not pull in the consideration of an aggressor. Techniques for image steganography consistently focus on keeping up the visual nature of an image while encoding a mystery message in it. This paper reports another calculation for LSB (Least Significant Bit) trade based image steganography for RGB shading images. The directional parts of inserting information are investigated to build up an improved LSB installing method. The outcomes report an improvement in image quality estimated by methods for PSNR and MSE.

R. Gupta and T. P. Singh [10] since the ascent of use of web on the planet security is turning into the real concern everywhere. Thus, making this thing unmistakable as a main priority engineers are consistently attempting to make web a sheltered domain for every one of the clients. Numerous calculation or procedures are proposed and they worked however as the interlopers are acting shrewdly to hack data engineers are likewise expected to concoct new methods to stop programmer's goals. According to the essential learning more is the PSNR worth and lesser is the MSE results are better along these lines, here in this paper creators are proposing another strategy by brushing three noteworthy security systems that is cryptography, steganography and watermarking that won't just conceal the data yet produce better outcomes for MSE. PSNR and Embedding limit still after the noise assault. The reason this paper is to give another system that will give better security to concealing information in an image and watermarked video.

Subhash Panwar [11] This paper examines about an idea on concealing the classified information in an image which is called as Image Steganography. Moreover, it utilizes a procedure known as Cryptography to improve the quality of security. Steganography shrouds the information and makes it hard to comprehend whether it really exists or not. Image Steganography explicitly alludes to concealing the information inside a spread image. Cryptography intends to change the information so that its significance is unidentifiable. Steganography when utilized alone does not ensure the security of information, so it is utilized alongside Cryptography. Steganography has its applications in fields which require a larger amount of security, for example, web based banking, protection and insight and so forth. Image Steganography is accomplished utilizing Modified LSB. Changed LSB utilizes a specific condition to supplant the bits of the private information at any rate noteworthy piece position of the pixels in the image.

## VI. PROPOSED WORK

The proposed concept implements the secure system of stegno image sending with the noise reduction, and integrity validation of the image and the text message. The steps which is performed in the total system of the communication is described in the following algorithm,

The algorithm for the secure communication,

Step 1: Register the user using the credentials used to identify the unique user.

Step 2: Login the system using the username and password.

Step 3: Select the Image which will act as carrier.

Step 4: Enter the text which is to be hidden.

Step 5: Enter the Key which will be used for encryption of the text to be hidden in the image, the AES algorithm will be used for the encryption of the text.

Step 6: Calculate the MSE and PSNR (note: simulation of the salt and pepper noise addition is done)

Step 7: Select the Receiver whom the message is to be sent and the unique message id is generated with all details saved in the database.

Step 8: SHA code for the text embedded is generated and stored in the database, MD5 code of the image containing the text is generated and stored in the database.

Step 9: At the receiver end, the receiver login with the credentials.

Step 10: The receiver will able to access in the message in the receive message section.

Step 11: Access the message received, to check the integrity of the image when the Md5 with the database MD5 for the image.

Step 12: Reduce the noise using the median filter.

Step 13: Enter the key to extract the message from the stegno image.

Step 14: Generate the SHA for the extracted text and validate it with the SHA sent for the text hidden, it is stored in the database.

Step 15: After all the validation the text is accepted.

Step 16: Stop.

## VII. IMPLEMENTATION

The process of the communication of the data starts with the registration of the user. This form is used to register the new user and details which are entered from the user are username, password and phone number. The unique constraints for the table are the user name and phone number , if they already exists then the corresponding error message will be shown to the user to indicate the error otherwise the record will be stored in the database. The database which is used for this purpose is MS SQL Server. Now , after the registration the next step is to ready the data which is to be sent, here we will select an image in which the data is to be hidden. The fig 4 shows the form which is used to hide the data into the image , in this the user has to first select the file in which the data is to be hidden , then we have to specify the text which is to be hidden in the image, the option is required to be checked if the user wants to encrypt the text in the image. If the user check the option of encrypted the text in the image, then the password is required to be specified for that.

After specifying the text and password, once we get the message that the text is successfully hidden, the next step is to save the file, and the file can be saved with any name and location.

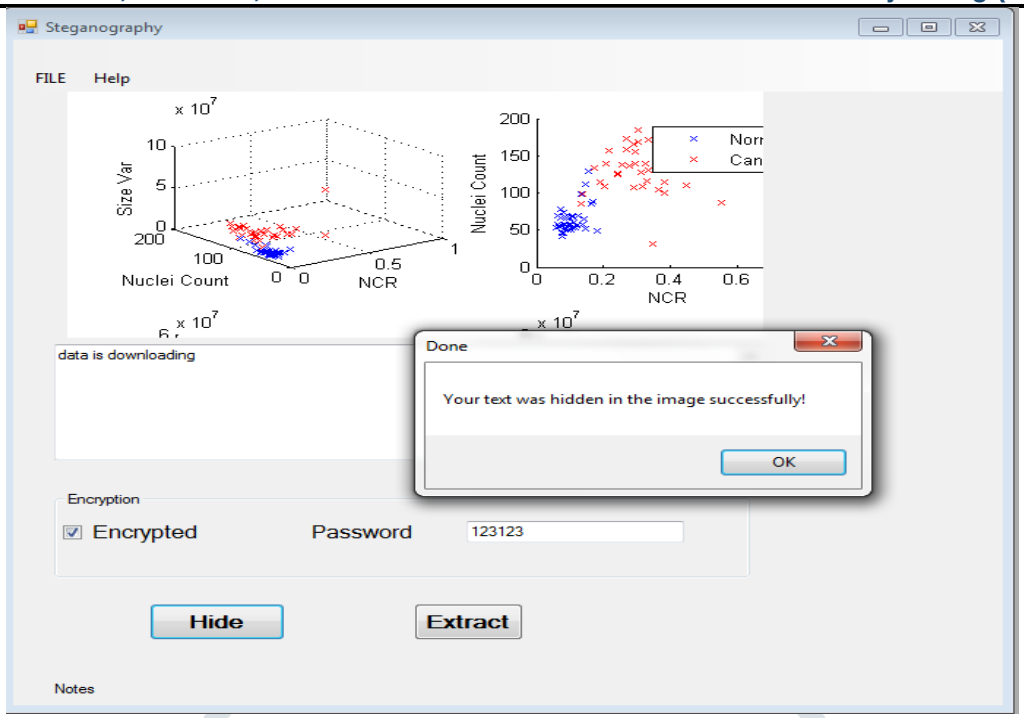


Fig 4. Hiding Text

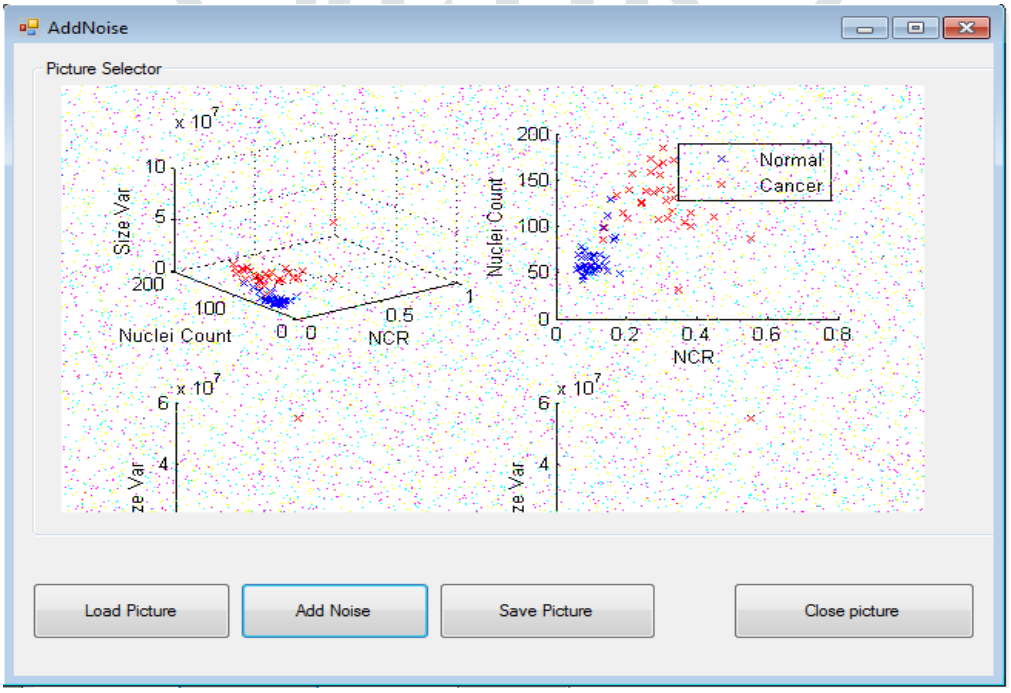


Fig 5. Noise Simulation

After the addition of the noise, it requires to save the file. Then after we save the file, we will generate the MD5 hash of the image which we are sending. Now the next steps is to generate the MD5 hash for the image which we are sending, the form which is used for generating the MD5 hash is shown in the fig 4.5. This form first selects the picture and then when the picture is loaded in the form. We have to click on the generate hash, the MD5 will get generate and will get stored in the database. Then the extraction process will be performed at the receiver end. The receiver end is shown in Fig 6.

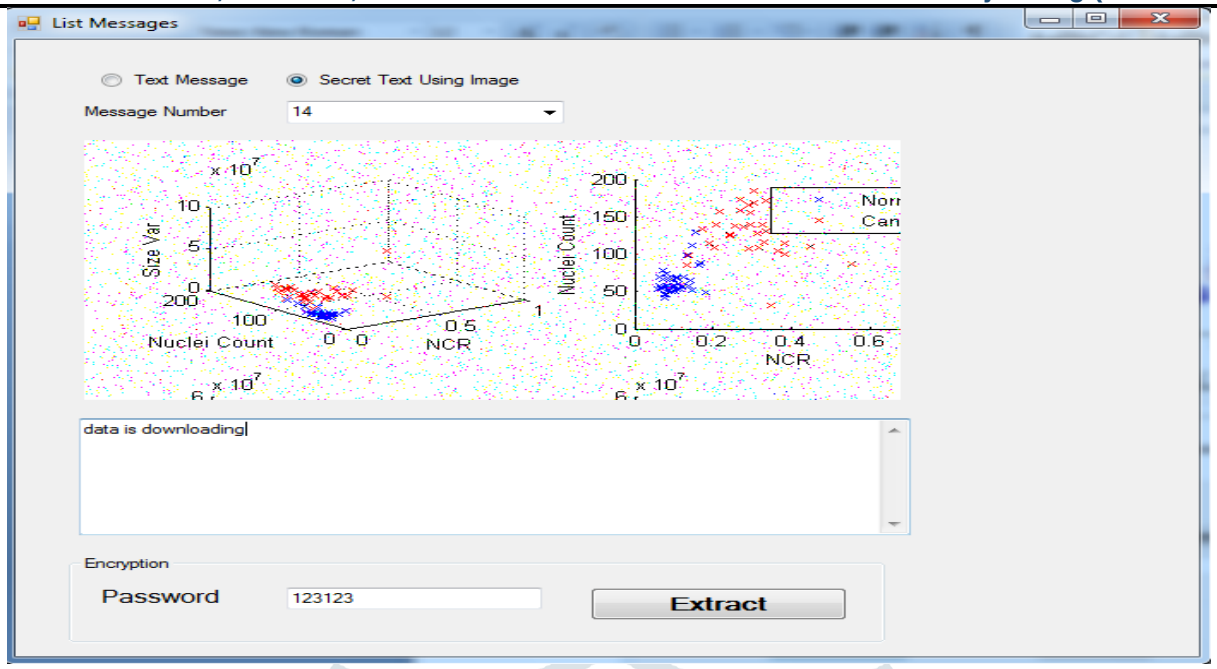


Fig 6. Extraction of Data

## VIII. Result Analysis

The calculation of the MSE and PSNR values is shown in this table. The MSE value should be lower after applying the median filter and the PSNR value should be higher after applying the median filter.

Table 1. MSE and PSNR value table

| Samples | Before Noise | Applying Median Filter Proposed Work |
|---|---|---|
| Duck | MSE 331.59<br>PSNR 22.9 | MSE 41.82<br>PSNR 31.9 |
| Power | MSE 246.04<br>PSNR 24.25 | MSE 0.842<br>PSNR: 48.90 |
| Gang | MSE 240.8<br>PSNR 24.34 | MSE 32.6<br>MSNR 33.02 |

## IX. CONCLUSION

Steganography methods for putting away information such that it shrouds the presence of them. Steganography used to complete shrouded exchanges.For model, Governments are keen on two sorts of correspondence of concealed information: first, which supports national security and second, which does not. Steganography bolster the two kinds, likewise business have comparative worries, about competitive innovations for new advancements or items data. Obviously, utilizing steganography to impart significantly lessens the danger of data spillage. Organizations exploits another type of steganography, called watermarking. Watermarking is mostly used to distinguish and involves concealed exceptional piece of data inside a medium without contacting the medium. The proposed work gives the information correspondence framework, which utilizes the steganography and the cryptography with the approval of images and the content shrouded utilizing the MD5 and SHA. The framework likewise works in the portion for the noise expulsion to decrease the system aggravations of sign which influences the information moved. The noise filtration is finished utilizing the middle channel approach. The outcomes which are gotten are very amazing.

## References

1. Neha Rani and JyotiChaudhary, “Text Steganography Techniques: A Review”, International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7- july 2013
2. Swati Gupta and Deepti Gupta, “Text -Steganography: Review Study & Comparative Analysis”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), 2011
3. ChintanDhanani and KrunalPanchal, “Steganography using web documents as a carrier: A Survey”, International Journal of Engineering Development and Research (IJEDR), ISSN: 2321-9939, 2013
4. S. Low, N.Maxemchuk, J.Brassil, L. O'Gorman, 1995. ”Document marking and identification using both line and word shifting”, Proceedings of the 14th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 95.

5. Krista Bennett, “Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text”, CERIAS Tech Report 2004-13.
6. Mohammed J. Bawaneh, Atef A. Obeidat,A Secure Robust Gray Scale Image Steganography Using Image Segmentation,Journal of Information SecurityVol.7 No.3, April 2016
7. Mohit Sharma,”Secure Message Transfer using Image Steganography”,Imperial Journal of Interdisciplinary Research (IJIR) 2016.
8. Arora, Aman & Pratap Singh, Manish & Thakral, Prateek & Jarwal, Naveen.,"Image steganography using enhanced LSB substitution technique,Research Gate,2016
9. Sugathan, Sherin," An improved LSB embedding technique for image steganography",researchgate,2016
10. R. Gupta and T. P. Singh, “New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters,” doi: 10.1109/IIH-MSP.2013.134 Proc. 2014 Int. Conf. Contemp. Comput. Informatics, IC3I 2014, pp. 475–479, 2014.
11. Subhash Panwar, Shreenidhi Damani, Mukesh Kumar,"Digital Image Steganography Using Modified LSB and AES Cryptography",International Journal of Recent Engineering Research and Development (IJRERD) ,2018