How to Cite:
Chaitanya, K., Prasanth, M., Saisrinivasreddy, S. V., & Kumar, S. K. (2022). Securing of aes based on secure hash algorithm for image steganography. *International Journal of Health Sciences*, *6*(S2), 1489–1499. https://doi.org/10.53730/ijhs.v6nS2.5107

Securing of aes based on secure hash algorithm for image steganography

Kakarla Chaitanya
Department of Electronics Communication Engineering, Vel Tech Multi Tech Dr Rangarajan Dr Sagunthala Engineering College Chennai, India
Email: kchaitanyareddy11@gmail.com

Prasanth. M
Department of Electronics Communication Engineering, Vel Tech Multi Tech Dr Rangarajan Dr Sagunthala Engineering College Chennai, India
Email: prasanthbharath2000@gmail.com

Saisrinivasreddy. V
Department of Electronics Communication Engineering, Vel Tech Multi Tech Dr Rangarajan Dr Sagunthala Engineering College Chennai, India
Email: vemurusaisrinivas@gmail.com

Senthil Kumar. V
Department of Electronics Communication Engineering, Vel Tech Multi Tech Dr Rangarajan Dr Sagunthala Engineering College Chennai, India
Email: senthil6038@yahoo.co.in

***Abstract*---**In this paper we tend to square measure handling Steganography victimization SHA-256 algorithmic program within the past we tend to used LSB algorithmic program. LSB(Least vital Bit) it's totally different results on 1bit and 2bit models .The use of additional bits affects the smoothness of image on stego image . Message is tough to recover if the image is subject to attack like translation and rotation. it's simple to decode to the hackers(other than WHO we tend to sent) .Message is well lost if image is subject to compression like JPEG, however solely such image kind is accepted by this algorithmic program. thanks to these drawbacks we tend to square measure moving to SHA-256(Secure Hash Algorithm), it's a scientific discipline hash additionally called digest .It enhances the extent of security in concealment of covert information exchange and data concealing .It generates a singular 256 bits (32 bytes) code of a text ,more secure than different common hashing algorithmic program. it's quick to calculate, immune to preimage and second preimage attacks and collision resistant. LSB algorithmic program has additional

International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696X © 2022.
***Corresponding author**: Chaitanya, K.; Email: kchaitanyareddy11@gmail.com*
Manuscript submitted: 27 Jan 2022, Manuscript revised: 18 Feb 2022, Accepted for publication: 09 March 2022

probabilities to be decrypted has it's coded with prime quantity combination therefore it is decoded simply. Whereas in SHA we tend to code with hash perform therefore it takes million of key combination to decode the code while not the correct key .So we tend to square measure victimization SHA-256 algorithmic program for image Steganography(encryption and decryption).

***Keywords*---**image steganography, algorithm, securing, decryption.

Introduction

Steganography is the popular one in every of the solutions to firmly transform information by concealing information in image. The information likely to hide in steganography is text or image. some algorithms for image primarily based steganography like, Chaos , International encoding algorithmic program (IDEA) , Advanced encoding customary (AES) , encoding customary (DES) , Message Digest five (MD5) , Bit Stream Ciphers , Secure Hash algorithmic program , etc are planned in recent times a number of these algorithms like AES, DES, and plan square measure sensible for tiny quantity {of information|ofknowledge} however not sensible for large data sets as these algorithms involve excessive computation and needed quick process machines. Similarly different algorithms like MD5, SHA square measure supported scientific discipline hash technique that use a hash key of sixteen computer memory unit. The excessive use of pictures on web is useful in secure info sharing. This tells about the requirement for individuals to safeguard from their pictures andthe secret information or belongings.

Encryption and Decryption Process

In this part initial a sender sends a info to different aspect from the protection to send info safely. So initial of all sender converts the info into cipher text that is one layer protection to the given info which cipher text converts into hash code with hash perform construct victimization SHA-256 algorithmic program which supplies second layer protection to {the info|theknowledge|the data} and with the assistance of steganogrphy construct the sender inserts the hash code into a image known as stego image with user outlined key to lock the codes information safely. After finishing the method sender sends the information to receiver, at the receiverside (decryption method) the reverse process of encoding takes place. Thestego image obtained from receiver is decoded with key given by sender and victimization hashing perform hash code is decoded and also the obtained cipher text is decoded by victimization reverse method of encoding.Finally we tend to get the knowledge from sender.

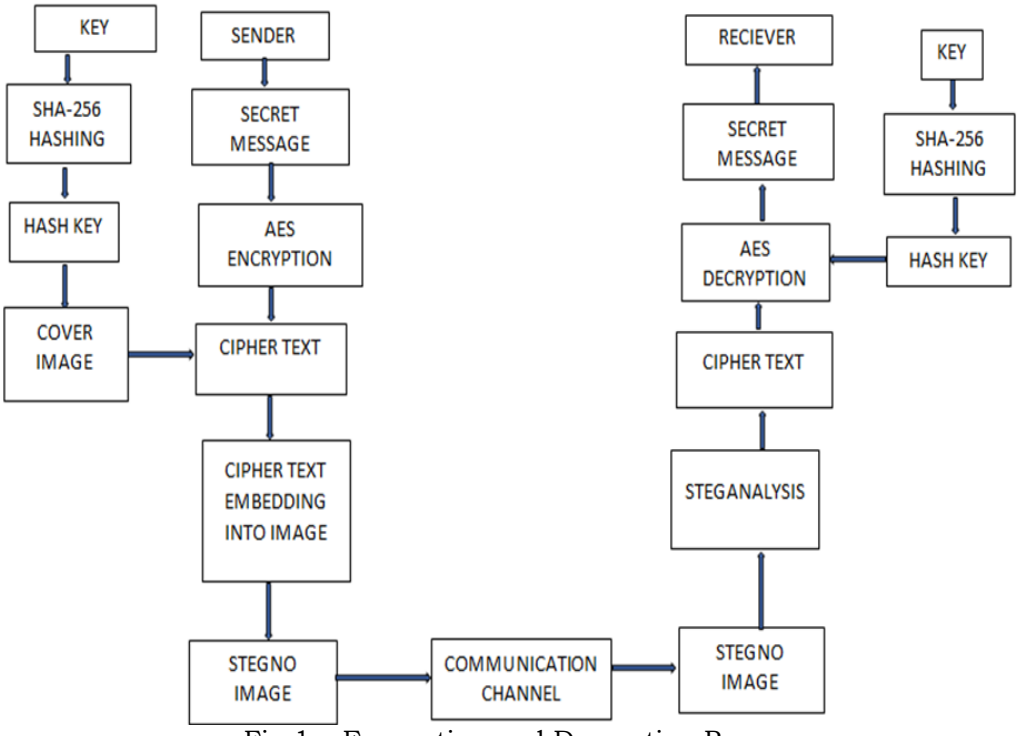


Fig-1a: Encryption and Decryption Process

EmbeddingData in Image and Creating Stego Image

At early stage throughout the beginning method initial and formost we want to enter a text of any length what we want to send. Then we want to outline a key either public or non-public.Now we want to enter the duvet image file with extension and path.Finally we want to engraft the image with hash code (secured information) from SHA algorithmic program by victimization python language we tend to get the stegoimage.Thisstego image is prepared to send vital info safely from one finish to a different finish.

Extracting Information from Stego Image

At the beginning of this method we tend to receives a stego image with a key(public or private).Then we want to perform stegoanalysis on the stego image to get the hash code. After obtaining the hash code we want to convert these into decoded type by victimization hashing technique with hash functions.After obtaining decoded info it's like cipher text then by victimization python language we tend to covert these cipher text into plain text.Finally these plain text contains the secured info received from different finish.

Interface Flowchart

Interface diagram shows the coding and secret writing method involves within the method. In coding method secret info from sender is protected with hash techniques and steganogrphy techniques with a constitutional key to secure the

given info .In secret writing method the hash code within stego image is obtained with key outlined by user and so converts it into plain text to recover the information from the sender.

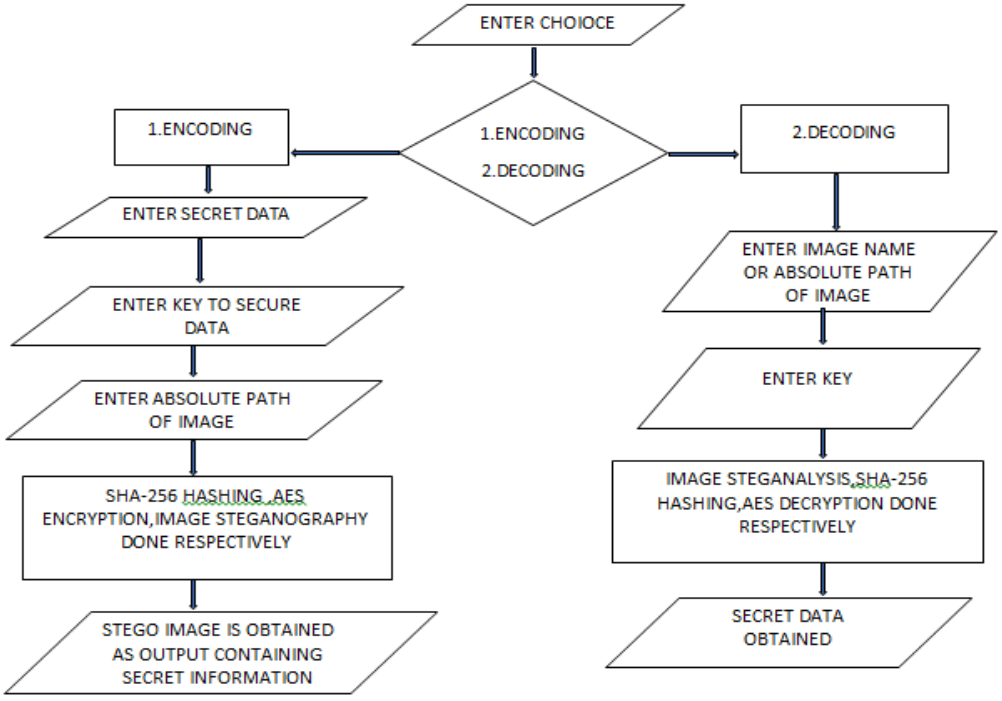


Fig-1b: Interface Flowchart

Encryption Process

Encryption method consists during this comes has three steps. First step consists of changing personal info into cipher text. Second step consists of changing cipher text into hash code victimization SHA-256 algorithmic program Third step accommodates compounding the hash code and image with user outlined key.

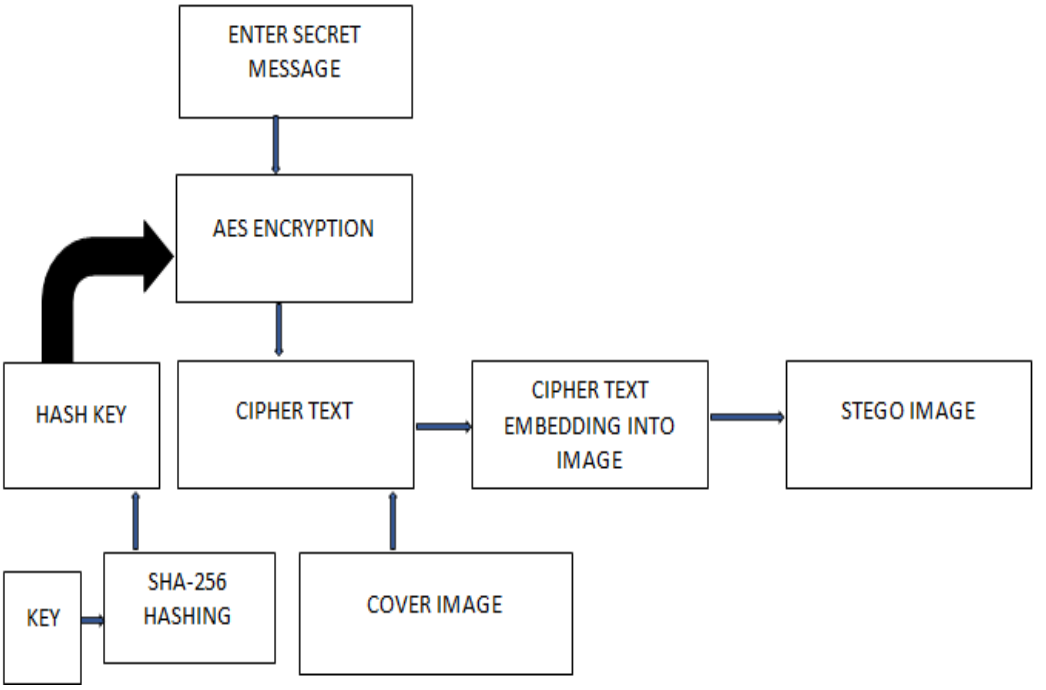


Fig-2: Encryption Process

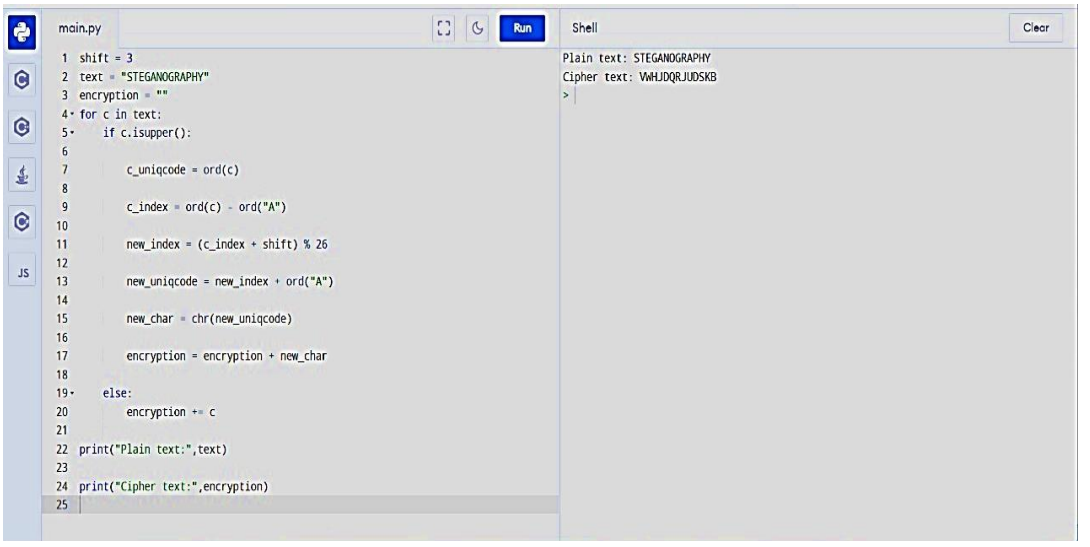
The process permits the consumer to implant their secret matter information in pictures all along a plan that will be hidden and doesn't damage or make an impression the standard of the primary figure.Target consumers of the likely structure square measure nation the one wish their information secure or protect their work form various or amerciable use. this method specifies Associate in Nursing careful means for dependable transfer of information. The likely approach is in a position to rule accompanying completely various file layouts for example Bitmap, jpeg/jpg, GIF.Proposed whole is in a position to load the above likely countenance file plans and treasure the likely piece of handbook into jpg/jpeg plan.

Converting Plain Text to Cipher Text Using Python

It is the unclear output of Associate in Nursing encoding algorithmic program. The term "cipher" is somecases used as an alternate term for ciphertext. Ciphertext isn't comprehensible till it's been reborn into plain text. In this code we tend to square measure changing traditional plain text into cipher text by victimization python language. For cryptography matter information within the image, a hash based algorithm is employed. The normalized purpose of victimization does changed the hash-based algorithmic program is to choose pixels willy-nilly to store chunks of computer data. The used algorithmic program willy-nilly generates a specific key that's after employed by the algorithmic program to come up with a pattern of pixels, wherever the information is keep. The good thing about victimization this type of approach is that every time information is coded the information is coded on a brand new possible pattern that creates the cryptography of information terribly economical. We use shift to

change the plain text {and we tend to and that we} use is upper() perform to examine whether the input text is in majuscule or not and so we use for loop for the encoding method. After execution the below code the pre entered plain text within the code converts into cipher text. We use 2 print statements for displaying the plain text and cipher text.

Output



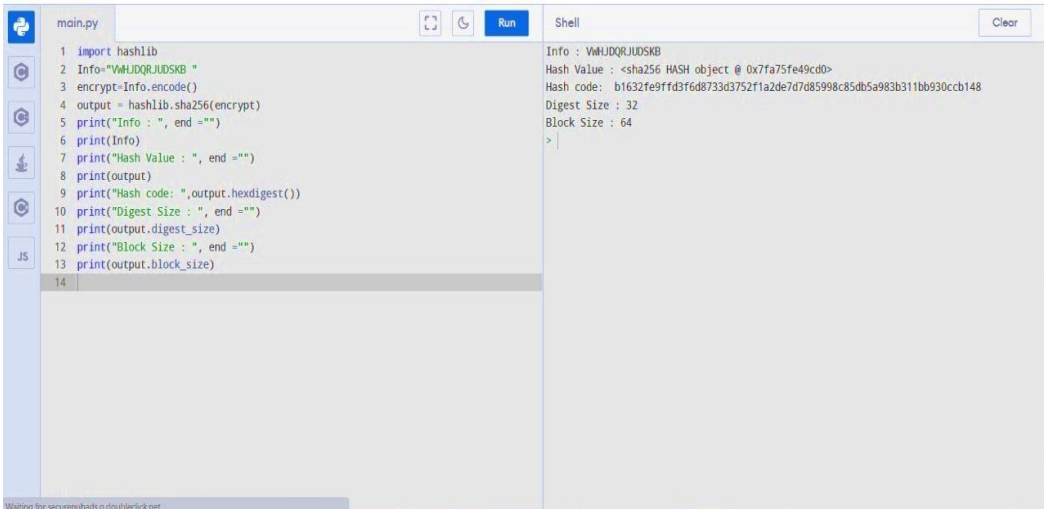
Converting Cipher Text in to Hash Code by Using Secure Hash Algorithm-256

To code secure hash algorithmic program initial we want to import hashlib perform. the foremost vital a part of the planned algorithmic program is that the used hashing technique. we've got used the right hashing as hash algorithmic program .For performing good hash technique we need to make sure with algorithm that we need to covert the given information into hash type code.An ideal mix-up act supports economical lookups by dawdling mix-up-answers from N to a hash-table. few implementations for all time mess functions square measure accessible.

we've received secondhand wildebeest exercise of hash act popular as 'gperf' that customarily generates good mix-up- functions for a mess-key. A 'gperf' generally based mix-up-function finds just individual} position all long a domain cheat just 1 probe. There square measure assortment of benefits of victimization good hash over various hash techniques. This hash algorithmic program is employed to convert the higher than cipher text into hash code that makes the knowledge safer. This algorithmic program acts as another layer of protection for the higher than cipher text that makes tough to decrypt the hint and it takes ample character set code combos to decrypt the knowledge.Soits safer thanks to send the knowledge. In the below code we tend to use hashlib perform with hashlibsha256 to code {the info|thedata|the info} given by user and print statements to print the positional representation system prices of the given

information and another print statements to grasp the digest value and block size. After execution the below code with success we tend to get the foremost secured hash code.

Output



Inserting the Hash Code in a Image Using Python

This code is employed to engraft the hash code (secret info from sender) that we tend to obtained by victimization sha-256 algorithmic program during a image then we tend to get astego image that sounds like the traditional image that concealing the given info as shown within the output below.In this code we tend to use cv2 module.ThisOpenCV may be a great tool for image process and performing arts pc vision tasks. it's Associate in Nursing ASCII text file library which will be wont to perform tasks like face detection, objection chase, landmark detection, and far additional. It supports multiple languages as well as python, java C++.We embody image dimensions and font size and image format(jpg or jpeg) and rbgcode.We declare a key within the code that is employed to decode the information that hidden within the image by receiver.

An recommendation connect is provided so a consumer will recommendation a (bmp, jpg, gif or jpeg) figure allalong which he/she desires to cover welcome/her individual facts for solitude functions. it's suggested that recommendation countenance should be medium judge to induce bigger results, still the questions complicated with the steganography plans square measure tangible characteristic, hardiness and file kind supports. Most wholes forbiddance appear expected compatible to file plan questions thats Most of the methods square measure for BMP kind files. however on the pc planet and on netting these types of pictures forbiddance seem expected stylish onccountof their proportion hottest layouts square measure jpeg/jpeg and g

Final Output of Encrypted Image

This is the output we get after executing the above code with secret informationembedded withimage.

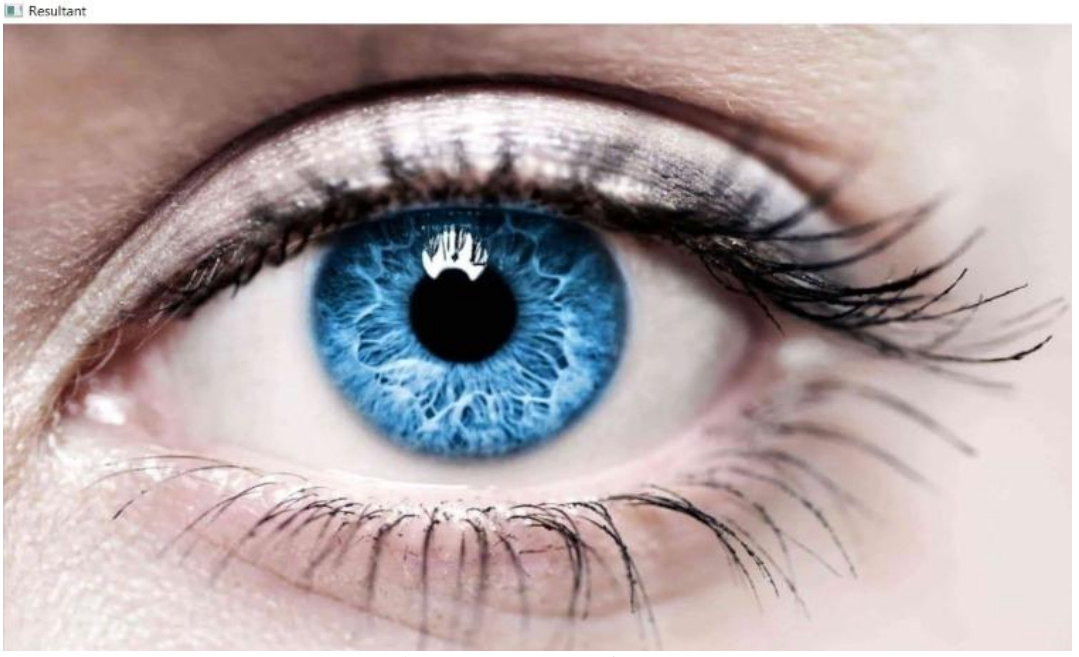


Fig-3a: Encrypted Image

Final Output of Decrypted Process

This is the output we get after executing the above code with secret information by using the key determined by the sender to decrypt the hash code embedded in the image.

Fig-3b:Decrypted Image

Decryption Process

Hash code is decrypted by victimization hashing technique with hash functions by comparison the code with numerous variety of combos. After decipherment of hash code we tend to get cipher text and that we convert these cipher text into plain text victimization python code mentioned below. During the decipherment method the reciever get the stego image through a line from sender.Thesestego image consists of personal info within the hash code format within the image.To recover the informataion within image we want to perform steganalyasis and that we get hash code.Then this hash code is decoded with hashing technique.The decoded type reborn into plain text that is straightforward to scan and understsandable to recieve aspect.

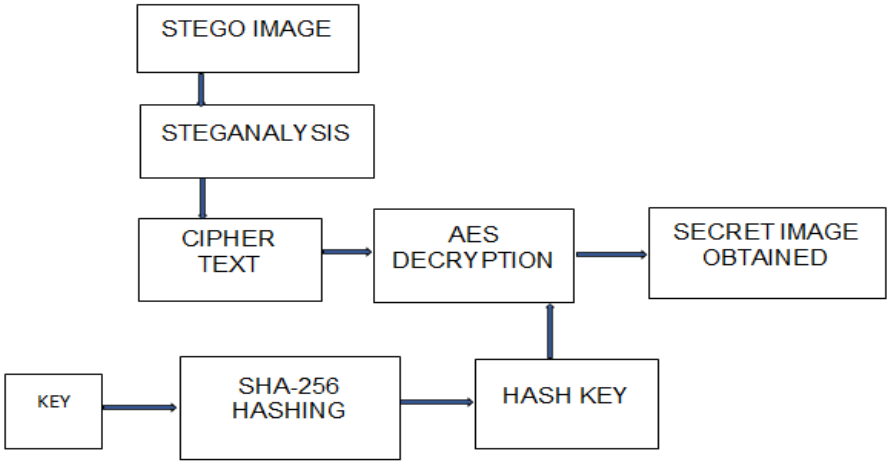


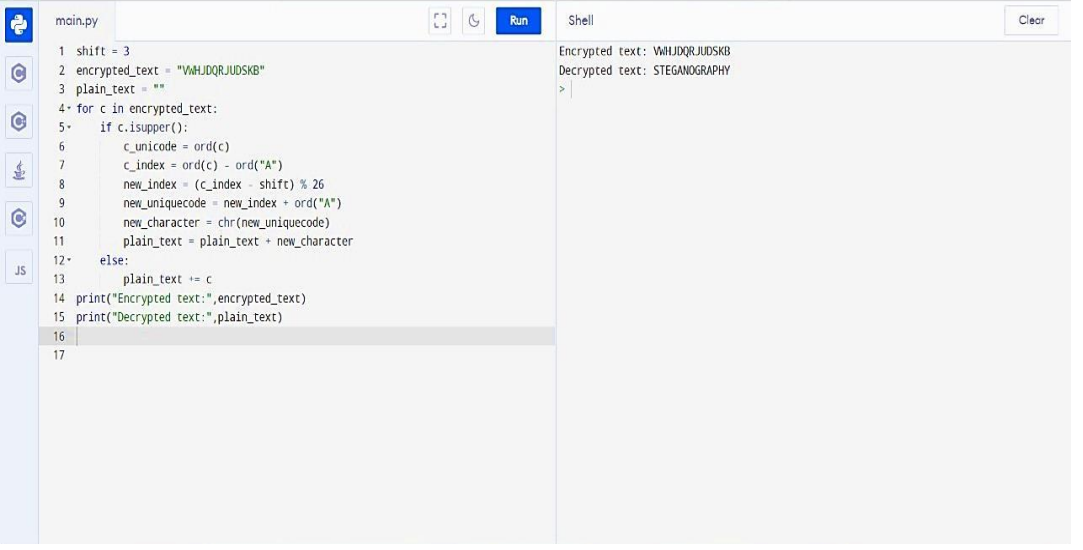
Fig-4: Decryption Process

Process to Decrypt Cipher Text

For signalingcode matter information within the figure, the messkey is employed that was produce to during the whole of secret word. By victimization the mix-up-key the secondhand algorithmic program produce the exactly alike pattern that was used concurrently with an activity of secret word. The pixels (red, green, vulgar data) principles of every position district whole scan one at a time and produce individualities concatenated to create an whole idea.This code is employed to decode the on top of cipher text that we have a tendency to get once decrypting the hash code.In this code we have a tendency to use shift to change the combos to rewrite the cipher text to create into plain text that we have a tendency to given at the beginning of the coding method.We use for loop for encrypted text and isupper() operate to see weather the given cipher text is in capital and that we use 2 print statements for displaying encrypted text and decrypted text.

Output

Finallywe get the word what we given at the beginning of the encryption process.



Summary and Conclusions

The devised method has sturdy capability to flip through dimensional information from a (bmp, gif, jpeg, and jpg) image and disguise figure and hide knowledge inside the figure while not unbinding the standard of the image. this method particularly everything for careful and secure knowledge action in pictures to construct achievable large-judge encryption and broadcast over net. The discharged approach is completely machine-reserved. we've likely the primary experiments with the correct hash generally {located} algorithmic program located approach for color countenance steganography. However, the secondhand algorithmic program will be upgraded to urge larger and correct(perfect) results,additional in close to future this technique of stegnography are going to be

utilized in each secret communications and in military functions, it'll be a brand new generation of secure communication as we have a tendency to use SHA algoritham throughout the embedding method.

References

1. 2004 Fridrich, Jessica; M. Goljan; D. Soukal .Delp Iii, Edward J; Wong, Ping W (eds.). "Searching for the Stego Key" (PDF). Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of multimedia system Contents VI.Security, Steganography, and Watermarking of multimedia system Contents VI. 5306: 70–82. Bibcode:2004SPIE.5306...70F. doi:10.1117/12.521353. S2CID 6773772.
2. 2001Pahati, OJ "Confounding Carnivore: a way to defend Your on-line Privacy". AlterNet. Archived from the first on
3. 2007Petitcolas, FAP; Anderson RJ; Richard Kuhn MG ."Information Hiding: A survey" (PDF).Proceedings of the IEEE.eighty seven.
4. 2019Osama F. Abdel Wahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf and Hanafy M. Ali, "hiding knowledge in pictures victimization steganography techniques with compression algorithms", Journal of analysis gate.
5. 2019Mustafa Sabah Taha, MohdShafryMohd Rahim, Sameer abdulsattarlafta, Mahomet Mahdi Hashi and Hassanain Mahdi Alzuabidi, "A short survey on Combination of steganography", Journal of analysis gate,
6. 2016A. Pradhan, K. Raja Sekhar and G. Swain, "Digital image steganography supported seven-way component worth differencing", Indian Journal of Science and Technology,.
7. 2017 M. Rahul, M. Malathi, N. Satish Kumar, R. Thamaraiselvan, “Enhanced Image Steganography victimization AES & SPIHT Compression”, International Conference on Innovations in info Embedded and Communication Systems .
8. 2015Khan Muhammad, Jamil Ahmad, Haleem Farman, Muhammad Zubair, “A novel image steganographic approach for activity text in color pictures victimization HSI color model”,
9. 2011 Riasat, Rubata&Bajwa, Imran.. A Hash-Based Approach for color Image Steganography. Proceedings - International Conference on laptop Networks and data Technology.
10. T.Morke1, "An summary of Image Steganography", Department of engineering science, University of African country|national capital}, South Africa
11. 2006S.Lyu and H. Farid, “Steganography victimization higher order image statistics, “IEEE Trans. Inf. Forens. Secure,.
12. 2002Dr. capital of Montana Handschuh, Dr. Henri Gilbert, “Security Level of Cryptography -SHA-256”, Issy-les-Moulineaux .
13. 2021 Basak, rattan & Chatterjee, Ritam& Dutta, Paramartha&Dasgupta, Kousik. Steganography in Color Animated Image Sequence for Secret knowledge Sharing victimization Secure Hash algorithmic program.
14. 2016.Pradhan. A, K. Raja Sekhar and G. Swain, "Digital image steganography supported seven-way component worth differencing", Indian Journal of Science and Technology,