International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362
IJARST

SECRET MESSAGE EMBEDDING IN VIDEO USING PYTHON

[1]Mr. J. MAHESH, [2]P. ADHITHI, [3]S. MURALI KRISHNA, [4]V. SANJAY
[1](Assistant Professor) , CSE. Teegala Krishna Reddy Engineering College, Hyderabad.
[2,3,4]B,tech , scholar , CSE. Teegala Krishna Reddy Engineering College, Hyderabad.

ABSTRACT

This project aims to implement video steganography in python using Django. Video steganography is a technique of hiding secret message within a video file without altering the visual quality of the video. In our project, we take the users secret information as a plain text and we converting into cipher text using AES Encryption. The method involves embedding the secret message in the least significant bit(LSB) of each pixel of each frame, the GUI will provide a user-friendly experience for selecting the videos and messages and display the output video containing the encrypted message.

1. INTRODUCTION

Internet is no longer safe to transfer sensitive information. The dependence of the people made the hackers to monitor the network and attack for sensitive information. The data is securely saved in our system might not be safe when we transfer it over the internet. Also, the system itself can be effected with virus, trojans and malwares in variety of ways. This leads to intrusion into the system and again loss of data. Therefore, security is the most important thing for the people since evolution of hacking. Steganography is the method of embedding the data into object where human sense cannot sense it [1]. This means the communication is accomplished in such a way that the message existence cannot be identified. The word cryptography in Greek can be shown as ‘Krypto’ means hidden and ‘graphene’ means to writing. Image Steganography A digital image or video is most secure way to carry the sensitive information through the internet using steganography. The image is captured using the camera, the light of the camera will sense the object which should be captured, and the will be displayed on the screen of the camera. Image is combination of the pixels; the resolution of the picture depends upon the pixel. Pixel is the minute are of illumination on a display screen. Human eyes cannot sense the pixels in the image.Pixel is made of three components. Three components of the pixel are Red, Green and Blue (R, G and B). Each pixel has depth of 24 bits that is 3 bytes [2]. Each component is of size one byte. Any color is formed by the combination of these three components. The byte value varies from 0 to 255. The color will be displayed based on the value of the bits, 0 is the darkest and 255 is the brightest.The size of the picture is given in the pixels, for example the size of the picture is 600*450, then the image is the combination of 2,70,000 pixels. pixel is made of three components which of each component is size of 8 bits, for example 11111111 00000000 00000000 is the pixel bits then the pixel will red in color. Depending upon the RGB values the pixel color will be changed.

2. LITERATURE SURVEY

The image protection in wireless channel is proposed in [7]. After embedding the data using LSB, the image is divided into blocks which is size of 8*8. The blocks are encrypted using double random phase encoding which converts into stationary noise. Using Fourier transformation, the image multiplied by random phase mask is converted to frequency domain from time domain and random phase mask is applied. Presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employ an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.the data to be transferred is encrypted using RSA algorithm. Using LSB the encrypted data is hidden inside audio object which provided high security to the data. The secret message is encrypted using Vernan cipher according to [10]. The data is embedded into the image using LSB. The authors used grayscale images. S-DES algorithm is used in [11] to encrypt the secret message to produce an array. The elements of the array are divided into 2 parts where first part contains 4 MSB's and other contains LSB's. The value of each pixel is transformed alphabets from A to P which is 0000 to 1111.

Requirement Analysis:

Functional Requirements:

These are the requirements that the end user specifically demands as basic facilities that the system should offer. All these functionalities need to be necessarily incorporated into the system as a part of the contract. These are represented or stated in the form of input to be given to the system, the operation performed and the output expected. They are basically the requirements stated by the user which one can see directly in the final product. 3 Reference [12] has introduced has given a hybrid approach for the security if the data that enhances the quality if the encryption. Used blowfish algorithm to encrypt the image to cipher image. Then the encrypted image is embedded using LSB technique in the cover image. Blowfish algorithm is lossless and highly secured encryption technique. [13] Mp3 file is used as a cover object. The secret message is encrypted using AES algorithm with the key generated by MD5 hash function. The encrypted data is embedded into mp3 files along with key code. The author uses space domain steganography in [14]. One image is embedded into another image. Using a key as a seed pseudo randomness is generated in the images. The pixel is selected and using column sequence and row sequence, the plane of secret image is divided into 16 pixels.

3. SYSTEM DESIGN

3.1 System Architecture

The proposed system is built around conventional three-tier architecture. The three-tier architecture for web development allows programmers to separate various aspects of the solution design into modules and work on them separately. That is, a developer who is best at one part of development, say UI development need not worry about the implementation levels so much. It also allows for easy maintenance and future enhancements. The three-tiers of the solution include:

¬ **The Layout:** This tier is at the uppermost layer and is closely bound to the user, i.e., the users of the system interact with it through this tier.

¬ **The business-tier:** This tier is responsible for implementing all the business rules of the organization. It operates on the data provided by the users through the web-tier and the data stored in the underlying data-tier. So in a way this tier works on data from the webtier and the data-tier in order to perform task for the users in agreement with the business rules of the organization.

¬ **The data-tier:** This tier contains the persist able data that is required by the business tier to operate on. Data plays a very important role in the functioning of any organization. Thus, persisting of such data is very important. The data tier performs the job of persisting the data.

The Model-View-Controller (MVC)

is an architectural pattern that separates an application into three main logical components: the model, the view, and the controller. Each of these components are built to handle specific development aspects .

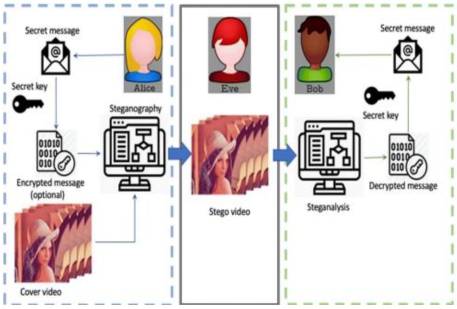


fig-1: encryption and decryption

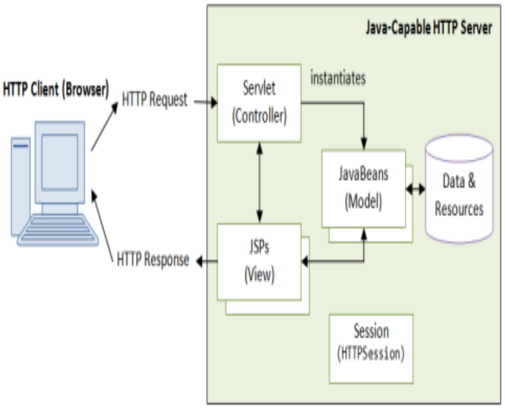


fig-2: techinal architecture

ACTIVITY DIAGRAM: Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-bystep workflows of components in a system. An activity diagram shows the overall flow of control. . Control flows connect actions, specifying the order of execution, while decision nodes enable branching based on conditions. Forks and joins manage parallel flows, and swim lanes partition activities among different entities for clarity

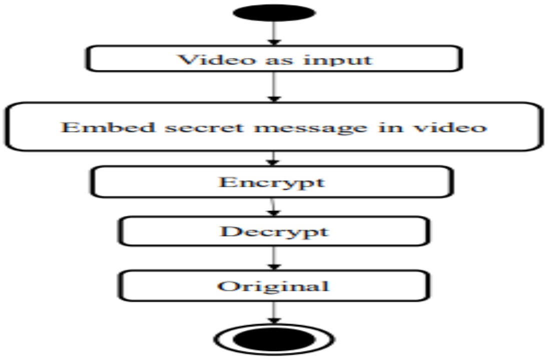
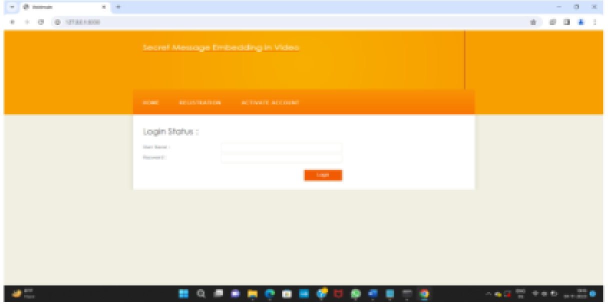
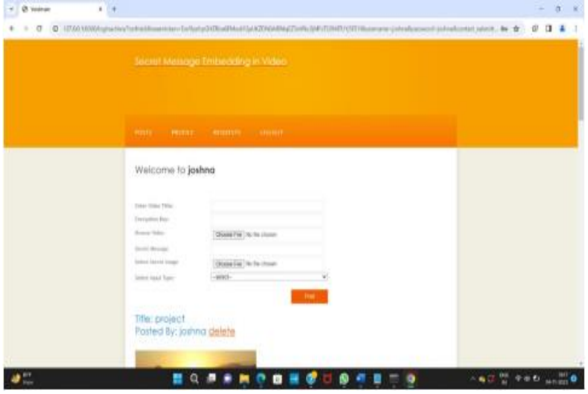


Fig-3: Activity Diagram

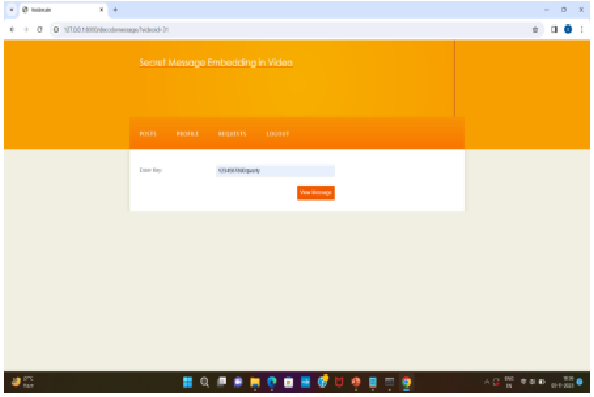
4. OUTPUT SCREENS



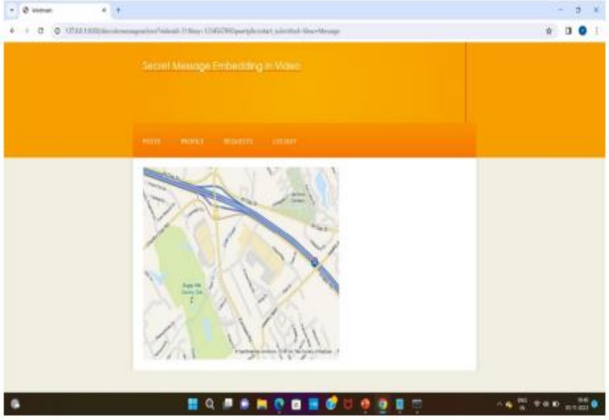
LOGIN: Here we validate Username and password on database.After validation a home page is displayed i.e.below screen,where the user can see all the encrypted posts that are posted by other users.



Post Encrypted Video: If the user want to send an encrypted message(image or text) then the user need to choose a cover video and the encrypted message along with a 16 digit security key. Toclick From the other end,the receiver login to the page by validating username and password.In order to get the secret message the receiver sends a key request to the sender



Decrypting the video: Once the key is received ,the 16 digit key is entered in the provided dialog box then clicks on to get the decrypted message.



5. CONCLUSION

we concluded that using crypto-steganography, one can achieve two levels of security. There will be no thirdparty interruption by using this technique because no one can even know that data is embedded into the image or video as there will be no noise created in the cover image. It provides high level of integrity and confidentiality of messages. There are numerous numbers of algorithms are developing to overcome the lags in the existing algorithms and enhancing the level of security of the data transmitted through the internet. Whereas there are many message detection techniques are developing simultaneously, still detection doesn’t guarantee retrieving all the information. Crypto steganography is the technique where we encrypt the data using the key and using that key, we are embedding the data in the pixels of the cover image pseudo randomly. Even though we are changing the bits of the components of the pixels of the image there will not be more distortion in the stego image, however there will be some distortion created that cannot be seen by human eyes. Furthermore, we are hiding the data in the noisy picture and transmitting so that data will be more secure. By this way the stego image will be same as the cover image. Numerous application areas are developing like the cloud security, online communication sites etc., the vision into the crypto steganographic principles will make us find vivid areas of application.

6. FUTURE ENHANCEMENT

Explore and implement advanced steganographic algorithms that offer better security and less perceptibility. Research and incorporate state-of-the-art techniques to embed and extract data efficiently. Integrate encryption techniques to secure the hidden information within the video. Implement compression algorithms to reduce the size of the embedded data, ensuring efficient use of storage. Implement more advanced encryption techniques to secure the hidden data. You could explore using stronger encryption algorithms or combining multiple encryption methods to enhance the security of the embedded information. Enhance the robustness of your steganography technique by incorporating error correction codes. This can help in recovering the hidden data even if the video undergoes some alterations or corruption. Develop a system that dynamically adjusts the amount of data embedded based on the characteristics of the video. This could involve adapting to changes in scene complexity, motion, or other factors to ensure a more robust and less detectable steganography process. Explore adaptive embedding techniques that adjust the hiding strategy based on the content of the video. This could involve modifying the embedding rate based on the video's characteristics to make the steganography more adaptable and less detectable. Optimize your implementation for real-time video steganography. This could involve parallel processing or other optimization techniques to embed and extract data efficiently without noticeable delays. Investigate the integration of deep learning techniques for steganalysis resistance. Train a neural network to detect hidden information in videos and use this knowledge to improve the steganography method to resist detection. Create a user-friendly interface for your steganography tool. This could include a graphical user interface (GUI) that allows users to easily select videos, set parameters, and perform the steganography process. Ensure that your implementation works seamlessly across different platforms and video formats. Consider making your code compatible with popular video editing software or platforms for wider usability. Perform security audits and vulnerability assessments on your steganography implementation. Identify and address potential weaknesses to make your system more robust against attacks.

7. REFERENCES

[1] SREELAKSHMI (2015, NOV 9). “Image steganography using LSB,” https://www.slideshare.net/SreelekshmiSree 1/image- steganographyusing-lsb (accessed: February 27, 2019).

[2] 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.

[3] Osuolale and A. Festus, “Secure Data Transfer Over the Internet Using Image Crypto Steganograph y.” in International Journal of Scientific & Engineering Research, 8(12), pp. 6-9, December 2017.

[4] S. Singh and V. K. Attri, “Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm “, in International Journal of Signal Processing, Image Processing and Pattern Recognition,Vol. 8, No. 5, pp. 259-266, 2015.

[5] R. Böhme, “Advanced Statistical Steganalysis information security and cryptography,” in New York, NY: Springer. DOI: 10.1007/978- 3- 642-14313-7, May 2010.

[6] K.S. Seethalakshmi, Usha. B, and Sangeetha. K. N, “Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography,” in IEEE Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.

[7] S. Bukhari, M. S. Arif, M.R. Anjum and S. Dilbar, “Enhancing security of images by Steganography and Cryptography techniques”, in IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016.

[8] R. Das, I. Das, “Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques”, in IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.

[9] A. Gambhir and S. Khara, “Integrating RSA Cryptography & Audio Steganography”, in IEEE ICCCA, 2016.

10] K. Joshi, R. Yadav, “A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication,” in IEEE ICIIP, 2015.