SECURING TEXT MESSAGE WITHIN A VIDEO USING LSB STEGANOGRAPHY AND RSA ALGORITHM

S C Yalla Reddy[1], N Abhishek[2], R Sai Vardhan[3], V Jagannadh[4], G Karthika[5].

[1,2,3,4]Student, Department of Computer Science Engineering, Gitam University ,Visakhapatnam.

[5]Assistant Professor, Department of Computer Science Engineering, Gitam University ,Visakhapatnam.

Guide - Mrs. G Karthika

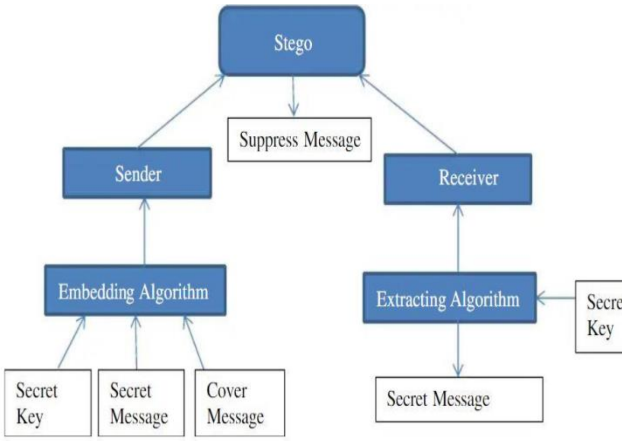
ABSTRACT

The Internet is the media because of which it is feasible to move information from one spot to somewhere else with exceptionally rapid. Be that as it may, it is exceptionally unsafe to move information over the web. Thus to keep up with protection and to keep an unapproved individual from extricating data steganography procedure is utilized. Steganography is the study of hiding restricted data. The restricted data is as text, picture, sound and video. This restricted data can be hiding in the text, picture, sound and video. Hiding privileged intel in a video document is called video steganography. In this task, one of the most outstanding secure steganography procedures (LSB) is introduced. With the development in advanced correspondence advances and the fast development of network transmission capacity, the Internet has ended up being an ordinarily involved channel for sending many reports for example, sound, video, picture, and message in advanced structure. Many practices have been offered and produced for giving the protected transmission of information. The focal point of the ebb and flow research is on the plan of data hiding procedures utilized for sending restricted information where computerized pictures are chosen as the cover-media. This part has distinguished the issues in the present picture steganography plans.

1. INTRODUCTION

Steganography is a strategy for sharing privileged data by making it subtle to non-verified clients. Steganography has been started from Greek word "Steganos" and illustrations. Steganos implies covered or stowed away and designs implies composing. Greek People utilized steganography to convey secret message through various strategies. Other strategy to keep up with security of data is Cryptography. Of which previous is for the most part utilized for validation furthermore, later is utilized for concealing message utilizing encryption. Steganography is fundamentally utilized in security applications like clandestine correspondence, legitimate fields and copyright Control. Security frameworks are basically zeroing in on insurance of privileged data by utilizing encryption or cryptography.

Cryptography gives security of data by modifying significance of data through scrambling or encoding by utilizing encryption key. Regardless of how break sealed is our encoded message, it will be weak all of the time to assault as interloper definitely knows the presence of privileged intel. Steganography is superior to cryptography as it hides the presence of mystery message from gatecrasher.



Since quite a while, individuals have been hiding information by various methods furthermore, varieties. The Golden age Greeks had first rehearsed Steganography by dissolving wax tablets and afterward recording the secret message on the basic wood. Wax was reapplied which gave the vibe of a new, unused tablet. This served their motivation of mystery message correspondence. Afterward, Germans created microdot innovation. These are photos of a printed particular size having the clearness of standard-sized typewritten pages where the message was neither stowed away nor encoded. It was too little to even consider causing to notice itself and consequently, helped in the transmission of a lot of information. Steganographic innovation comprised of undetectable inks during early WWII. Milk, vinegar, organic product juices and pee were the normal wellsprings of undetectable ink which obscured when warmed. The developing techniques in this field has ignited a unrest which delivers various plans to pass on a message furtively.

An undertaking was begun in Saudi Arabia at the King Abdulaziz City of science and innovation, to decipher a few antiquated Arabic compositions, which are accepted to have been composed 1200 years prior, to English which was with respect to secret composition. The upside of steganography in cryptography alone is the planned hidden data doesn't stand out to it as an object of examination. Clearly apparent encoded information, regardless of how tough they are, stir interest furthermore, may in them be implicating in nations in which encryption is illicit. Though cryptography is the act of safeguarding the substance of a message alone, steganography is worried about covering the way that a mystery message is being sent and its substance.

Steganography incorporates the covering of data inside PC records. In advanced steganography, electronic interchanges might incorporate steganographic coding within a vehicle layer, for example, an archive record, picture document, program, or convention. Media records are great for steganographic transmission in view of their huge size. For instance, a source could begin with a harmless picture document and change the shade of each 100th pixel to relate to a letter in the letters in order. The change is inconspicuous to the point that somebody who isn't explicitly searching for it is improbable to see the change.

2. LITERATURE SURVEY

In light of the exploration done by Engineering innovation and applied science research in February 2019, in this examination they have presented both the blend of Steganography and Cryptography on picture utilizing LSB Technique. Thus, to ad lib the system though in picture we can store restricted measure of information however a video is a bunch of different casings so we can conceal huge sum of information with in a video. Thus, we will involve video as a cover media. In Video Steganography we partition the cover video into edges and supplement information inside each outline as picture Steganography and afterward after we join every one of the casings in an request. Then, at that point, a stego video is made after that we extricate the information from the stego video. Top notch Steganographic strategy with PVD and Modulus work was an expansion of PVD based approach. This strategy initially computes the distinction esteem between two sequential pixels and afterward modulus activity was utilized to ascertain their leftover portion. The restricted information were inserted into the two pixels by adjusting their leftover portion. The concealing limit of the two back to back pixels relies on the distinction esteem taken. Lesser the distinction esteem smoother the region, so just less restricted information could be installed as well as the other way around. The strength of the plan was that it could incredibly diminish the perceivability of the secret information than the PVD technique. Since the plan utilized the rest of the two back to back pixels it was more adaptable. Nonetheless, a proviso exists in the PVD strategy. Surprising advances in the histogram of pixel contrasts uncover the presence of a mystery message. The altered pixels will be spread around the entire stego picture and many smooth locales gets sullied.

3. IMPLEMENTATION

In this paper, the philosophy we are utilizing for Cryptography is RSA and for
locking up the data in a cover media we will utilize LSB Steganography
strategy.

3.1 Types of Steganography:

In light of the condition, there are numerous strategies of encoding wherein picture decipherment is most well known method. Practically all advanced record organizations can be utilized for decipherment, yet the arrangements that are more appropriate are those with a serious level of overt repetitiveness. Overt repetitiveness can be characterized as the pieces of an article that give precision far more noteworthy than needed for the article's utilization and show. The excess pieces of an item are those bits that can be modified without the change being distinguished without any problem. Picture and sound documents particularly conform to this necessity, while research has likewise revealed other record organizes that can be utilized for data stowing away. It very well may be isolated primarily into four classifications:

Classifications of Steganography:

1. Audio/Video steganography
2. Text steganography
3. Convention steganography
4. Picture steganography

3.1.1 Audio/Video Steganography

In Audio/Video steganography, a mystery message is concealed in sound/video record. The double arrangement of sound/video document is somewhat varying from unique record which won't be quickly be distinguished by natural eyes. Least Significant Bit is most normally utilized in this class. A few sorts of Audio/Video steganography are:
I. Stage coding
ii. Spread Spectrum
iii. Reverberation stowing away

3.1.2 Text Steganography

Concealing data in text is generally the main strategy for steganography. In this kind of steganography, lock up data is concealed in a message. There numerous procedures are utilized such sequencing in which each person of mystery message is covered up a fix position of message or the paired worth of mystery message is concealed in twofold worth of text [8]. Microdots and utilization of additional void area are the illustration of text steganography.

3.1.3 Protocol Steganography

This term alludes to the method of installing data inside messages and organization control conventions utilized in network transmission. In the layers of the OSI network model there exist clandestine channels where decipherment can be utilized. An illustration of where data can be covered up is in the header of a TCP/IP bundle in certain fields that are either discretionary or are never utilized. This sort of method is utilized in network level to conceal the mystery message since there a field in IP header in TCP/IP suite or web for information stowing away due to which datagram becomes imperceptible. Banner, ID fields are utilized for Convention decipherment.

3.1.4 Image Steganography

Picture decipherment is a strategy which is utilized to conceal secret message inside an picture. The double pieces of mystery of message are concealed in the twofold of picture and this somewhat influences the forces of shading or splendor which isn't distinguishable by exposed natural eyes. There are numerous calculations which are utilized for picture however some of them are extremely complicated while some of them are basic. As expressed before, pictures are the most famous cover objects utilized for steganography. In the space of advanced pictures various picture document designs exist, the greater part of them for explicit applications. For these different picture record designs, different steganographic calculations exist. A straightforward picture steganographic model contains a unique picture, called cover(I) picture in which secret part confidential message/picture (M) is covered up and a stegokey (K) which is utilized to stow away the data as well as to remove. The reason for utilizing stego key is to give security. At last, after the steganographic interaction, a picture is gotten called stego-picture(S) in which pixel esteem is not the same as the pixel worth of unique picture however these progressions is minor to the point that it won't be quickly distinguish by natural eyes.

RSA ALGORITHM

RSA is a asymmetric-key cryptology that is broadly utilized for hidden information motion. In a asymmetric-key cryptology, the encipher key is asymmetric and particular from the unscrambling key, which is made mystery (private). A RSA client makes and distributes a asymmetric key in light of two huge indivisible numeri's, with an assistant worth. The indivisible numbers are kept mystery. Messages can be encoded by anybody, by means of the asymmetric key, however must be decoded by somebody who knows the indivisible numbers.

Qualities of RSA:

□ It is a public key encryption procedure.

□ It is ok for trade of information over web.

□ It keeps up with secrecy of the information.

□ RSA has high sturdiness as breaking into the keys by interceptors is very troublesome.

The keys for the RSA calculation are created in the accompanying manner:

1. Pick two particular indivisible numbers p and q. For security purposes, the whole numbers p and q ought to be picked aimlessly, and should be comparable in greatness yet contrast long by a couple of digits to make figuring harder.[2] Prime whole numbers can be proficiently found utilizing an essentially test. p and q are kept mystery.

2. Process $n = pq$. n is utilized as the modulus for both people in general and private keys. Its length, generally communicated in bits, is the key length. n is delivered as a component of the public key.

3. Process $\lambda(n)$, where λ is Carmichael's totient work. Since $n = pq$, $\lambda(n) = \mathrm{lcm}(\lambda(p), \lambda(q))$, and since p and q are prime, $\lambda(p)= \varphi(p) = p - 1$ and similarly $\lambda(q) = q - 1$. Henceforth $\lambda(n) = \mathrm{lcm}(p - 1, q - 1)$. $\lambda(n)$ is kept mystery. The lcm might be determined through the Euclidean calculation, since $\mathrm{lcm}(a,b) = |ab|/\mathrm{gcd}(a,b)$.

4. Pick a number e to such an extent that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; that is, e and $\lambda(n)$ are co-prime. e having a short piece length and little Hamming weight brings about additional productive encryption - the most ordinarily picked incentive for e is 2 16 + 1 = 65,537. The littlest (and quickest) an incentive for e is 3, yet entirely such a little an incentive for e has been demonstrated to be less secure in certain settings. e is delivered as a feature of the public key.

5. Decide d as $d \equiv e -1 \pmod{\lambda(n)}$; that is, d is the secluded multiplicative backwards of e modulo $\lambda(n)$. This implies: tackle for 'd' the condition $d\cdot e \equiv 1 \pmod{\lambda(n)}$; d can be figured proficiently by utilizing the Extended Euclidean calculation, since, much obliged to e and $\lambda(n)$ being coprime, said condition is a type of Bezout's character where d is one of the coefficients. d is kept mystery as the private key example.

Benefits of RSA

□ It is exceptionally simple to carry out RSA calculation.

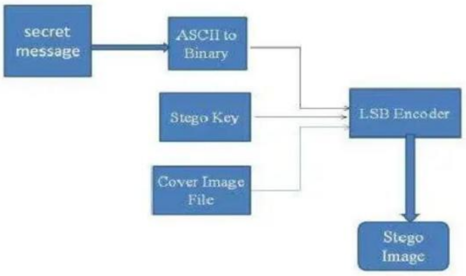
□ RSA calculation is free from any and all harm for sending secret information.

□ Breaking RSA calculation is undeniably challenging as it includes complex arithmetic.

□ Sharing public key to clients is simple.

LSB STEGANOGRAPHY

LSB Steganography is a steganography method where we conceal messages inside a picture by supplanting Least huge piece of picture with the picture and concentrate the RGB Values of a pixel and trade the last piece of RGB values with a genuine message bit. By changing the last piece of a pixel values, we can't see a lot of contrast with unique picture and stego image.



In a dark scale picture every pixel is addressed in 8 pieces. The last piece in a pixel is called as Least Significant piece as its worth will influence the pixel esteem exclusively by "1". Along these lines, this property is utilized to conceal the information in the picture. Assuming anybody have considered last two pieces as LSB bits as they will influence the pixel esteem just the pieces of message to be covered up. Here we partition a video into set of pictures and takes each of by "3". This aides in putting away additional information. The Least Critical Bit (LSB) steganography is one such method in which least huge piece of the picture is supplanted with information bit. As this strategy is helpless to steganalysis to make it safer we scramble the crude information previously installing it in the picture. However the encryption interaction expands the time intricacy, and yet gives higher security moreover. This approach is extremely straightforward. In this technique the most un-huge pieces of some or the bytes as a whole inside a picture is supplanted with a touch of the mystery message. The LSB inserting approach has turned into the premise of numerous strategies that stow away messages inside sight and sound transporter information. LSB inserting may even be applied in specific information areas - for instance, inserting a secret message into the shading upsides of RGB bitmap information, or into the recurrence coefficients of a JPEG picture. LSB installing can likewise be applied to an assortment of information arrangements and types. Hence, LSB installing is quite possibly the main steganography procedure
being used today.

LSB ENCODING ALGORITHM

First the first picture and the packed scrambled secret message are taken. Then, at that point, the encoded privileged information must be changed over into paired design. Double change is finished by taking the American Standard Code of Information Trade (ASCII) upsides of the person and changing over them into double design and creating stream of pieces. Also, in cover picture, bytes addressing the pixels are taken in single exhibit and byte stream is produced. Message pieces are taken successively and afterward are set in LSB bit of picture byte. Same system is followed till all the message pieces are set in picture bytes. Picture created is called 'Stego-Image'. It is prepared for transmission through the Internet. Calculation for concealing restricted information in Cover picture:

Step-1: Read the cover picture and mystery text data which is to be inserted in to the cover picture.
Step-2: Compress the privileged data.
Step-3: Convert the compacted restricted data into figure text by utilizing secret key shared by beneficiary and source.

Step-4: Convert packed scrambled instant message into twofold structure.
Step-5: Find LSBs of each RGB pixels of the cover picture.
Step-6: Embed the pieces of the privileged intel into pieces of LSB of RGB pixels of the cover picture.
Step-7: Continue the method until the restricted intel is completely concealed into cover record

LSB DECODING ALGORITHM

To start with, 'Stego-Image' is taken and single exhibit of bytes are produced as it was finished at the hour of encoding. The complete number of pieces of encoded privileged intel also, the bytes addressing the pixels of stego-picture are taken. Counter is at first set to 1, which thus gives the file number of the pixel byte where mysterious message bit is accessible in LSB. The cycle is gone on till definite count of mystery message bit is reached. After this, the piece stream of the message will be produced. 30 Available pieces are gathered to frame bytes with the end goal that every byte addresses single ASCII character. Characters are put away in message document which addresses the encoded implanted message. After that the unscrambling and decompression are to be performed.

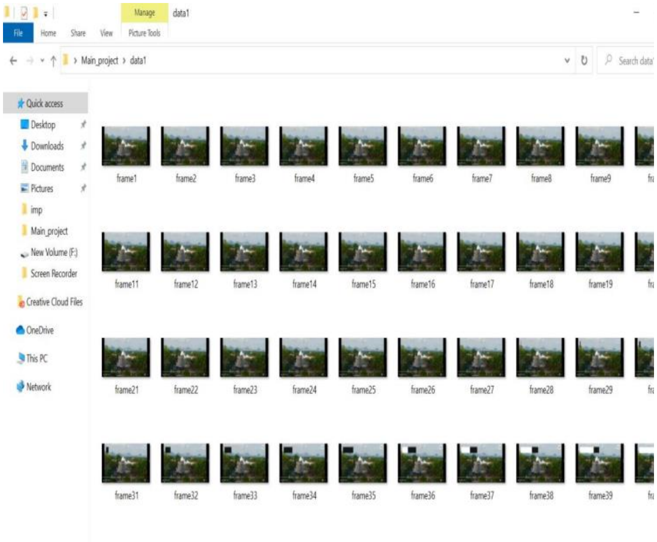
Calculation for interpreting privileged information from Stego picture:

Step-1: Read the stego picture.
Step-2: Find LSBs of each RGB pixel of the stego picture.
Step-3: Find and recover the LSBs of each RGB pixel of the stego picture.
Step-4: Continue the cycle until the message is completely removed from stego picture.
Step-5: Decompress the removed privileged information.
Step-6: Using shared key, unscramble privileged data to get unique data.
Step-7: Reconstruct the privileged intel

Right off the bat, we seek shelter video and the mystery message as information. Furthermore, Next, we take the secret message and presently take every one of the person in the message and ascertain the ascii upsides of every single person in the message and afterward after Encrypt the message utilizing RSA Algorithm and afterward it gives the code message and convert that code message to 12 Bit parallel and afterward "concat" all the code message double numbers. Also, Now Take the cover video and catch the video utilizing the cam=cv2.videoCapture(video_file_name) and afterward remove every one of the edge from the video utilizing cam.read() and afterward separate every one of the pixel from the picture and the believer pixels to Binary and afterward trade LSB Bit of pixel double with information bit paired. These cycles until the information bit become invalid and then, at that point, save the encoded outlines in information envelope. And afterward we pack every one of the encoded edges to a video utilizing cv2.videoWriter() and afterward we remove the sound from the video and apply that sound to above encoded video utilizing MoviePy.editor module Presently we will get the stego video, this stego video is ship off the recipient. What's more, Now the beneficiary will partition the stego video into set of edges and store them in one envelope Presently we take every one of the edge from the organizer made at the beneficiary end utilizing cv2.imread(filename) and we recover the pixels and afterward we get the code message from the pixels and afterward we unscramble the message utilizing RSA with the keys given by the source and afterward convert to the message.

4. RESULTS

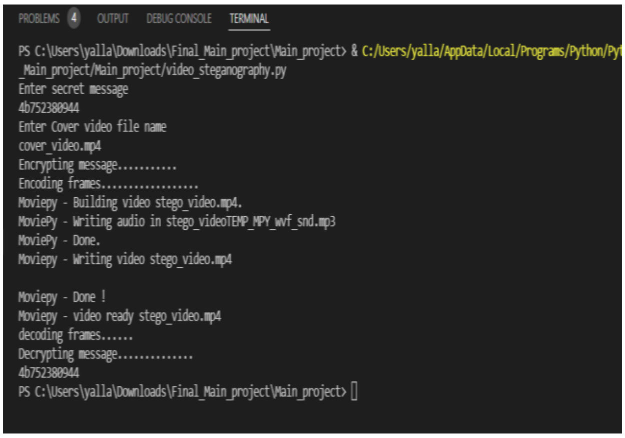
At source side, we accept input as cover video and mystery message and furthermore, we are doing encryption utilizing RSA Algorithm and encoded message is
encoded into the casings of the video and the stego-video is shipped off the
Receiver.



At beneficiary side, we remove the casings of the encoded video and afterward we
remove the encoded message from the casings and afterward we unscramble the
Message

At last, the beneficiary has gotten similar mystery message of shippers
with practically no interference.

5. OUTPUT



```
PS C:\Users\yalla\Downloads\Final_Main_project\Main_project> & C:/Users/yalla/AppData/Local/Programs/Python/Pyt
_Main_project/Main_project/video_steganography.py
Enter secret message
4b752380944
Enter Cover video file name
cover_video.mp4
Encrypting message...........
Encoding frames..................
Moviepy - Building video stego_video.mp4.
MoviePy - Writing audio in stego_videoTEMP_MPY_wvf_snd.mp3
MoviePy - Done.
Moviepy - Writing video stego_video.mp4

Moviepy - Done !
Moviepy - video ready stego_video.mp4
decoding frames......
Decrypting message..............
4b752380944
PS C:\Users\yalla\Downloads\Final_Main_project\Main_project> []
```

6. CONCLUSION

The new development of web clients has expanded the requirement for safety of data. decipherment is the method utilized for security of information. Video decipherment is utilized for concealing the privileged data (text, picture and video) in video document. So this project presents the different strategies of video steganography. decipherment is a truly fascinating subject and outside of the standard cryptography and framework organization that the vast majority of us manage consistently. Steganography can be utilized for buried correspondence. We have investigated the cutoff points of steganography hypothesis and practice. We printed out the improvement of the picture steganography framework utilizing LSB way to deal with give a method for secure correspondence. A stego-key has been applied to the framework during installation of the message into the cover picture. This steganography application programming accommodated the reason to how to utilize any kind of picture arrangements to concealing any sort of documents inside them. The expert work of this application is in supporting any kind of pictures without need to change over to bitmap, and lower impediment on record size to stow away, as a result of utilizing greatest memory space in pictures to conceal the record. Since old times, man has tracked down a longing in the capacity to convey clandestinely. The new blast of exploration in watermarking to safeguard licensed innovation is proof that steganography isn't simply restricted to military or secret activities applications. Steganography, similar to cryptography, will assume an expanding part in the fate of secure correspondence in the "advanced world".

7. REFERENCES

1. DIGITAL IMAGE PROCESSING (4th Edition), Rafel C. Glonza Lez, Richard E. Woods

2. INTRODUCTION TO CRYPTOGRAPHY (2nd Edition), Johannes A. Buchman

[3] Das, S., Das, S., Bandyopadhyay, B., & Sanyal, S. (2011). Steganography and Steganalysis: different approaches. arXiv preprint arXiv:1111.3758.

[4] Budhia, U., Kundur, D., & Zourntos, T. (2006). Digital video steganalysis exploiting statistical visibility in the temporal domain. Information Forensics and Security, IEEE Transactions on, 1(4), 502-516.

[5] Dengre , A. R., Gawande, A. D. Deshmukh, , A. B.(June, 2013). Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI
video . International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2(6), 2319 – 4847.

[6] Wajgade, V. M., & Kumar, D. S. (2013). Enhancing Data Security Using Video Steganography. International Journal of Emerging Technology and Advanced Engineering, 3(4), 549-552.

[7] Ramalingam, M. (2011). Stego Machine–Video Steganography using Modified LSB Algorithm. World Academy of Science, Engineering and Technology, 74,502 505.

[8] Ahmed, Z. H. (2014). Comparison of data hiding using LSB and DCT for image (Doctoral dissertation, Universiti Tun Hussein Onn Malaysia).

[9] Shukla, C. P., & Singh, A. K. (2014). Secure Communication with the help of Encryption in Video Steganography.Current Trends in Technology and Sciences.ISSN: 2279-0535. Volume: 3, Issue: 6