Enhanced Security System Using Video Steganography

Mayur Rangade
Department of Computer Engineering
Modern Education Society
College of Engineering Pune
mayurrangade@gmail.com

Akshay Randive
Department of Computer Engineering
Modern Education Society
College of Engineering Pune
akshayrandive111@gmail.com

Gaurav Nagpure
Department of Computer Engineering
Modern Education Society
College of Engineering Pune
gpnagpure@gmail.com

Ashish Hulwan
Department of Computer Engineering
Modern Education Society
College of Engineering Pune
ashishhulwan@gmail.com

***Abstract* — In today's world large amount of data is transferred over the internet. Sometime this data contain confidential information of a person. Hackers can easily get this information and misuse it. There are numerous techniques accessible which have its own preference and inconveniences. In proposed framework we clarify a strategy for steganography in which information in the content organization is covered up into the video document. Information to be covered up might be in pdf record, word document or writing content. Video record can be of any arrangement like mp4 and 3gp and so on. Video document goes about as a spread record. We are going to use scene change algorithm and RSA algorithm for steganography. This method minimizes the attention of hackers as they assume that video is transferring. This results in secure transmission of data.**

Keyword-Steganography, Cryptography, Encryption, Decryption, RSA

I. INTRODUCTION

The progression of Technology, Internet, and Information Sharing has had both positive and negative effects. One of negative effects was the vast increment in new Information Threats to beat this dangers there a need of framework which will give security to Information that streams over the Internet, so we chose to grow such framework. Encryption programming shields web associated PCs from saltines and other online interlopers. The innovation is broadly used to encode charge card data, ledger numbers and other sort of monetary records so they can send securely and safely over the web. Secure a great part of the scholarly substance that is advertised on the web, for example, music, Videos, articles, and programming, confining its accessibility to paying clients. This framework shrouds the data while sending the imperative and private archives in video documents; it will be imperceptible for the third individual. This framework is useful for the barrier and security offices sending and getting the private matters in crisis circumstances.

By and large steganography system is connected where the cryptography is inadequate [1]. The steganography structure includes the spread archive (picture, sound, component et cetera) and the puzzle message that is concealed inside the spread record by applying steganography the riddle message is covered and Stego record is made which is same as spread picture and undetected or unaltered Steganography (fromGreekSteganos, "Spread/covered up", and graphein, "to compose") is the workmanship and exploration of conveying in a way which conceals the presence of the correspondence [1].

Cryptography (from Greek kryptós, "concealed", and gráphein, "to form") is, generally, the examination of technique for changing over information from its typical. Reasonable structure into a boundless game plan, rendering it confounded without puzzle taking in, the art of encryption. The specialty of guaranteeing information (plain substance) by evolving it (scrambling it) into a garbled. Organization is called figure content. Simply the people who have a puzzle key can disentangle (or decipher) the message into plain substance. Mixed messages would some be able to of the time be broken by cryptanalysis, in like manner called code breaking, though current cryptography methodologies are in every practical sense unbreakable. Cryptography scrambles the genuine message that is being sent. This security instrument uses numerical arrangements and computations to scramble data into incomprehensible substance. It must be decoded or unscrambled by the social affair that has the related key [2].

A Goals And Objectives

1. To produce security tool based on steganography techniques.
2. To explore techniques of hiding data using encryption module of this project
3. To extract techniques of getting secret data using decryption module.

II. LITERATURE SURVEY

In [3] paper, proposed a development approach for element information insurance utilizing LSB and half breed approach. Steganography is the craft of conveying a message by installing it into interactive media information. The proposed strategies for supplanting maybe a couple or three LSB of every pixel in video outline and apply Advance encryption standard (AES). It turns out to be exceptionally troublesome for interloper to figure that a picture is covered up in the video as individual edges are extremely hard to examine in a video. In this perception crest to flag commotion proportion (PSNR) is grater for 1 bit LSB substation when contrasted with 3 bit LSB substation so when number of LSB substation bit expanded then security level is additionally expanded and perception connection coefficient has the worth r=1 if the two picture are totally indistinguishable, r=0 on the off chance that they are totally uncorrelated and r=-1 on the off chance that they are totally hostile to related for instance in the event that one picture is the negative of the other. In [4] paper we review different steganography plans for concealing the information. The principle objective of steganography is to convey safely in a totally imperceptible way so that nobody can recognize the transmission of a shrouded information. In this paper we examine the idea driving the steganography by depicting what is steganography and the terms that are identified with steganography. This paper gives the steganography strategies for picture steganography, sound steganography, video steganography, and content steganography that are utilized to insert the data in computerized media. The two most essential parts of steganography framework are the nature of stego article and the limit of the spread media. By investigating this paper, analysts can develop a superior steganography way to deal with expansion the PSNR esteem and to diminish the MSE. Framework are the aggregate expense of VPS is much less expensive than DSRC based ETC framework, it's anything but difficult to setup another toll region or evacuate the old ones, exchange time won't be the issue. Impairments consolidates High precision essential for vehicle arranging in ETC applications, issues connected with GPS signal blackouts, it is more troublesome in the coordinating procedure between the charge and authorization data, so the VPS framework needs more post-handling employments so as to diminish the jumble disappointment.

Researchers have completed diverse techniques for information and data security to finish secret correspondence. Steganography is a methodology for covering the secret messages into the conveyor medium, for instance, picture, sound, element et cetera steganography strategy is generally requested into three rule sorts specifically, system misusing picture design, technique installing in recurrence area and technique in spatial domain[5].

In [6] paper, a spatial area procedure for LSB Matching Revisited calculation (LSBMR) has been proposed, where the mystery data is implanted in the spread casings. LSB Matching Revisited (LSBMR) calculation chooses the inserting areas as indicated by the span of mystery message and the contrast between two back to back pixels in the spread picture. For implanting rates is lower, just more honed edge locales are utilized while keeping the other smoother districts as they seem to be. In the proposed approach, LSB Matching Revisited calculation is utilized to install the mystery message into the video. Henceforth a lot of information can be inserted furthermore safeguarding higher visual nature of stego pictures in the meantime. The proposed technique is broke down as far as both Peak Signal to Noise Ratio (PSNR) contrasted with the first cover Video and additionally the Mean Squared Error (MSE) measured between the first and steganography records arrived at the midpoint of overall video outlines.

III. METHODOLOGY

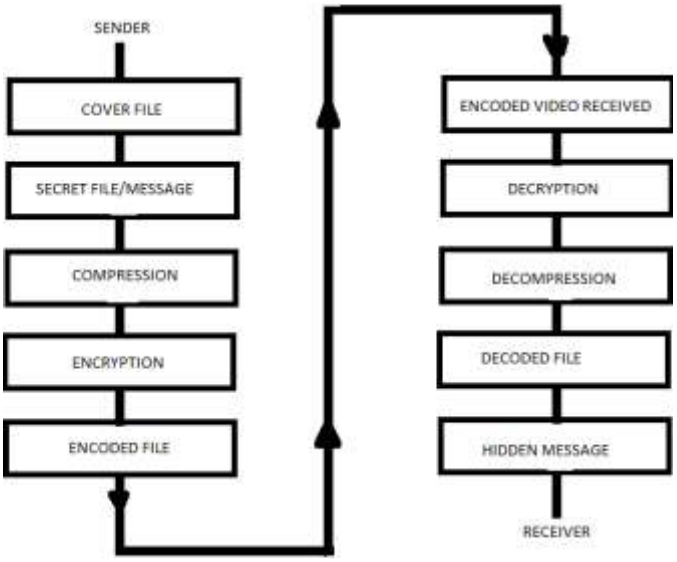


Fig 1: **System Architecture diagram**

In our proposed system user selects a cover file which is video of any type. After that user select a secret file which he wants to hide for secure transmission. Secret file is text file of any format such as doc file, pdf file, typing text etc. After selecting cover file and secret file user enter the secret key .After entering secret key user hit the encryption button .After that encrypted file is generated. This encrypted file user can send to intended receiver. Receiver on receiving this file decrypts the file using our software. For that purpose key is required which is entered by the sender. After entering the key receiver receive the secret file.

1. DES Algorithm

DES is a usage of a Feistel Cipher. It utilizes 16 round Feistel structure. The square size is 64-bit. However, key length is 64-bit, DES has a powerful key length of 56 bits, since 8 of the 64 bits of the key are not utilized by the encryption calculation (Capacity as check bits as it were).

General Structure of DES is depicted in the following illustration:

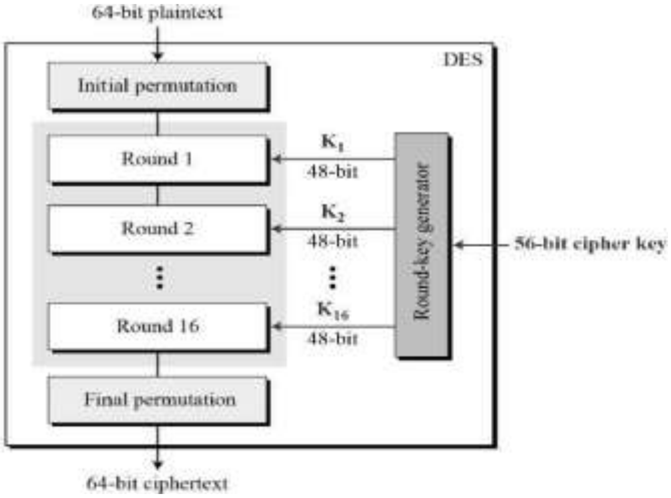


Fig 2: **DES Algorithm**

Since DES is based on the Feistel Cipher, all that is required to specify DES is

- Round function:- The heart of this cipher is the DES function, f. The DES Function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.
- Key schedule:- The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.
- Initial and final permutation:- The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no Cryptography significance in DES.

2. Triple DES Algorithm

Before utilizing 3TDES, client first produce and disperse a 3TDES key K, which comprises of three distinct DES keys K1, K2 and K3. This implies the real 3TDES key has length 356 = 168 bits. The encryption scheme is illustrated as follows

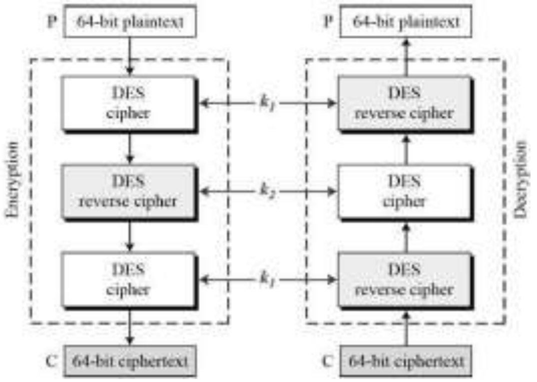


Fig 3: Triple **DES Algorithm**

The encryption-decryption process is as follows

- Encrypt the plaintext blocks using single DES with key K1.
- Now decrypt the output of step 1 using single DES with key K2.
- Finally, encrypt the output of step 2 using single DES with key K3.
- The output of step 3 is the cipher text.
- Decryption of a cipher text is a reverse process. User first decrypt using K3, then encrypt with K2, and finally decrypt with K1.

Because of this outline of Triple DES as an encrypt–decrypt–encrypt procedure, it is conceivable to utilize a 3TDES (equipment) execution for single DES by setting K1, K2, and K3 to be the same quality. This gives in reverse similarity DES. Second variation of Triple DES (2TDES) is indistinguishable to 3TDES with the exception of that K3is supplanted by K1. At the end of the day, client scramble plaintext obstructs with key K1, then decode with key K2, lastly encode with K1 once more. In this manner, 2TDES has a key length of 112 bits.

Triple DES frameworks are fundamentally more secure than single DES, however these are plainly a much slower handle than encryption utilizing single DES.

3. RSA Algorithm

RSA is the principal calculation referred to be appropriate for marking and in addition encryption, and was one of the primary incredible advances out in the open key cryptography. RSA is generally utilized as a part of electronic trade conventions, and is accepted to be adequately secure given adequately long keys and the utilization of a la mode usage.

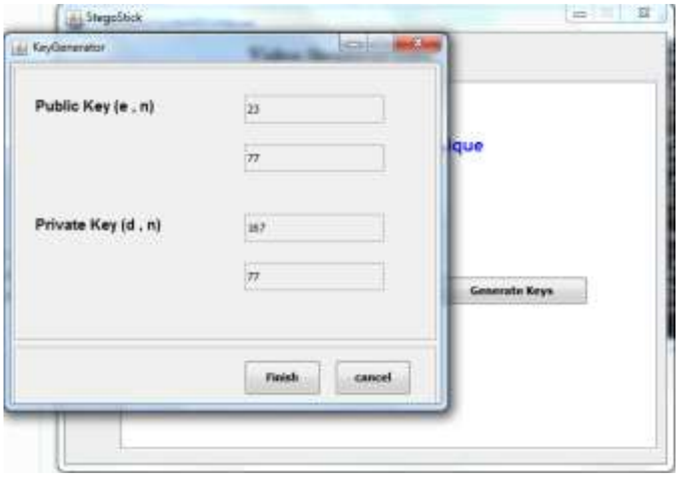
Ventures for RSA calculation as takes after:

1. Create two huge irregular primes, p and q, of roughly equivalent size such that their item n = pq is of the required piece length, e.g. 1024 bits.
2. Figure n = pq and (phi) f = (p-1)(q-1).
3. Pick a number e, 1 < e < phi, such that gcd(e, phi) = 1.
4. Figure the mystery type d, 1 < d < phi, such that ed = 1 (mod phi).
5. General society key is (n, e) and the private key (d, p, q). Keep all the qualities d, p, q and phi mystery. [We lean toward once in a while to compose the private key as (n, d) since you require the estimation of n when utilizing d. Different times we may compose the key pair as ((N, e), d).]

Example This is the original algorithm.

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute f (n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < f (n) and e and n are co-prime. Let e = 7
- Compute a value for d such that (d * e) % f (n) = 1. One solution is d = 3 [(3 * 7)% 20 = 1]
- Public key is (e, n) =) (7, 33)
- Private key is (d, n) =) (3, 33)
- The encryption of m = 2 is c = 27 % 33 = 29

The decryption of c = 29 is m = 293 % 33 =2



Public Key (e , n): 23, 77

Private Key (d , n): 167, 77

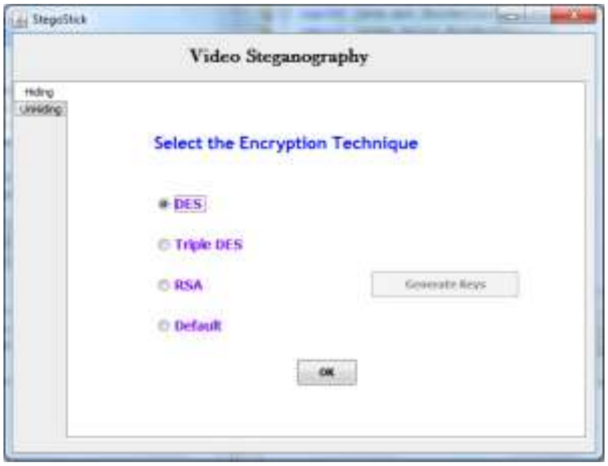
***Fig 4: RSA* Algorithm**

IV. SYSTEM MODULES

Modules Description:

Input Module:

The Input Module is planned accordingly a way that the proposed framework must be equipped for taking care of an information configurations, for example, if the client wishes to shroud any picture design then it must be good with all typical picture arrangements, for example, jpg, gif, bmp, it must be likewise perfect with video organizations, for example, .avi, .flv, .wmf and so forth.. Furthermore it must be good with different record designs, so that the client can have the capacity to client any organizations to conceal the mystery information.



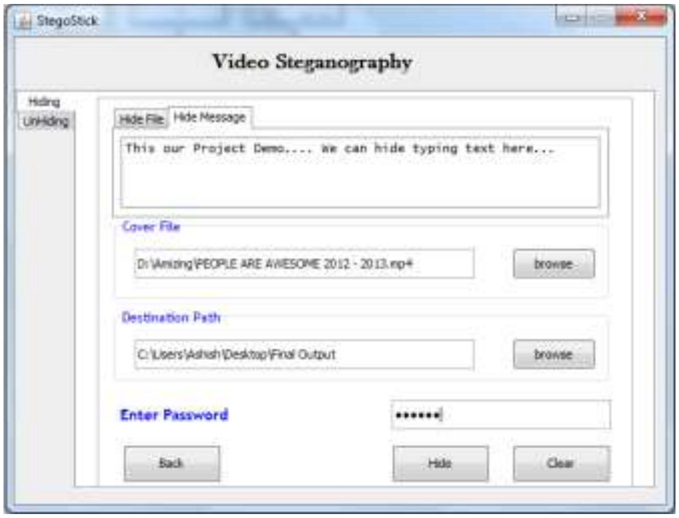
Select the Encryption Technique

● DES
○ Triple DES
○ RSA
○ Default

Fig 5: Input Module

Encryption Module:

In Encryption module, it comprises of Key document part, where key record can be indicated with the watchword as a unique security in it. At that point the client can sort the information or else can transfer the information additionally however the skim catch, when it is tapped the open record exchange box is opened and where the client can choose the mystery message. At that point the client can choose the picture or video document through another open record discourse box which is opened when the spread record catch is clicked. Where the client can choose the spread document and afterward the Hide catch is clicked so that the mystery information or message is covered up in spread record utilizing Forbidden Zone Data Hiding Technique.



This our Project Demo.... We can hide typing text here...

Cover File: D:\Amazing\PEOPLE ARE AWESOME 2012 - 2013.mp4

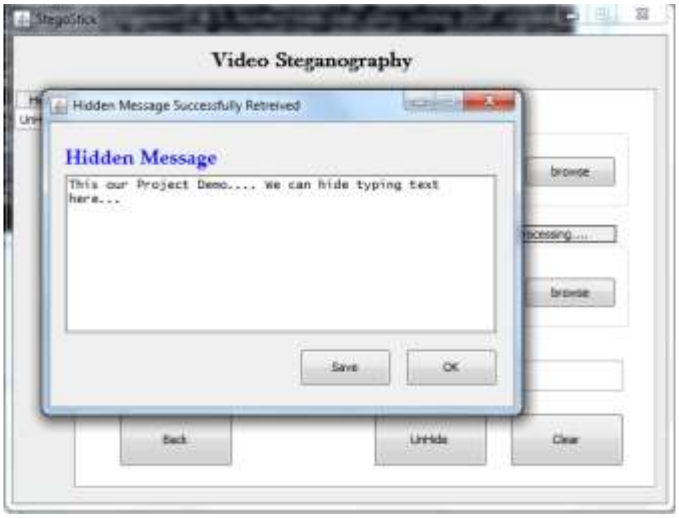
Destination Path: C:\Users\Ashish\Desktop\Final Output

Enter Password: ••••••

Fig 6:* Encryption *Module

Decryption Module:

This module is the inverse all things considered as Encryption module where the Key document ought to be likewise determined same as that of encryption part. At that point the client ought to choose the encoded spread document and afterward ought to choose the concentrate catch so that the concealed message is shown in the content region determined in the application or else it is extricated to the spot where the client indicates it.



```
This our Project Demo.... we can hide typing text
here...
```

Fig 7:* Decryption *Module

V. ADVANTAGES

1. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser.
2. In the business world steganography can be utilized to shroud a mystery substance equation or arrangements for another creation.
3. Military can also use steganography to keep their communications secret and to coordinate attacks.

CONCLUSION

Steganography particularly joined with cryptography, is a capable device which empowers individuals to impart without conceivable busybodies notwithstanding knowing there is a type of correspondence in any case. These strategies utilized as a part of the Exploration of steganography have propelled a great deal over the previous hundreds of years, particularly with the ascent of PC time. In spite of the fact that the methods are still not utilized all the time, the potential outcomes are inestimable. A wide range of systems exist and keep on being created, while the methods for distinguishing shrouded messages likewise progress rapidly.

REFERENCES

[1] Nutzinger,M.C.Fabian, and M.Marschalek. ”Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”. In Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP), 2010 Sixth International Conference.

[2] Kumar.B.,D.,Bhattacharya,P.Das,D.Ganguly and S.Mukherjee,” A tutorial review on Steganography”, International Conference on Contemporary Computing (IC3 2008), Noida,India,August 7-9,2008,pp.105-114.

[3] S. Khosla and P. Kaur, “Secure data hiding technique using video steganography and watermarking”, International Journal of Computer Applications Volume 95– No.20, June 2014,pp no (0975 – 8887) .

[4] R. Bahirat and A. Kolhe, “Overview of secure data transmission using steganography,” International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014).

[5] Abbas Cheddad,Joan Condell,Kevin Curran,Paul Kevitt,”Enhancing Steganography In Digital Images”.Proc.Canadian Conference on Computer and Robot Vision.

[6] H. Gupta and S. Chaturvedi, “Video steganography through lsb based hybrid approach,” IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014,pp no(99-106).

[7] K. N. Choudry and A. Wanjari, “A survey paper on video steganography,” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, pp no.2335-2338,.

[8] McGraw-Hill, “The java complete refernece,” tech. rep.