EFFICIENT DATA HIDING IN ENCRYPTED VIDEO USING CRYPTOGRAPHY

[1]Madhan.S, [2]Manimekala.M, [3]Punithavallai.K,[4]Suganya.V
[1]Assisstant Professor, [2]Student, [3]Student,[4]Student
[1,2,3,4]Department of CSE
[1,2,3,4]University College of Engineering-Thirukkuvalai, Tamil Nadu, India

Abstract : Video data hiding is a very important research topic. Security of information is major concern of information technology and communication. This project introduces elliptical curve cryptography and Least Significant bit substitution technique for hiding data in video file. In this project data hiding a form of cryptography embeds data into digital media for the purpose of identification, annotation. These algorithms are a basic algorithm of encryption and decryption for data hiding. The framework is tested by all kind of videos such as .mp4, .3gp, .avi etc., and gets successful output for all video data hiding process. The proposed scheme used by security, while hiding the video to provide security for encrypts and decrypt process. The simulation results show that the process of hiding the video by security.

IndexTerms - **Video Data hiding, Encryption, Decryption, Decryption, Security, RSA.**

I. INTRODUCTION

The Steganography is of Greek source and means "with this or unseen writing". Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Steganography is implemented in different fields such as military.

Industrial applications. By using loss less steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files .Lately, there has been growing interest in implementing steganographic techniques to video files as well as audio files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files and audio files. Image-based and video- based steganography techniques are mostly classified into spatial domain and frequency domain based methods. The main aim of steganography is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major difference between this process and the other process of secret exchange of in sequence because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information. However, in steganography, the existence of the information in the sources will not be noticed at all. the majority steganography job have been approved out on descriptions, video clips, texts, music and sounds. For video stream

Usually being accessible in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression. This is an unnecessary saddle best avoided. If the constraint of strict compacted area steganography is to be met, the steganography wants to be embedded in the compressed domain. Nowadays, there are large amount of video watermarking algorithms been proposed. Some of them are applied for compressed video. To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid. parallel to cryptography and steganography may undergo from the attack method (steganalysis). Much of the research work in the field of steganalysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding. Another major stream is based on the concept of blind steganalysis, which is formed by blind classifiers. The classifier should be trained to learn the differences between cover and stego-image features at first. In this paper, we propose a secure purse video steganography architecture taking account of steganalysis module, operated in a closed-loop manner to enhance the anti-steganalysis capability of the stego video with data embedded steganography.

II LITERATURE SURVEY

In this paper [1] sound is there in digital image throughout image acquirement, code, transmission, and processing ladder Noise is very difficult to remove it from the digital images without the prior knowledge of noise model. The advantage of this paper is a complete and quantitative analysis of noise models available in digital image. Disadvantage of this paper is cannot be compressed.

In this paper [2] this paper concentrates on the aspects and approaches of image hiding techniques and cryptosystem for digital images. Data hiding can be divided into two categories such as digital watermarking and steganography. The advantage is we can hide the data in image. Disadvantage is it is not perfect image.

In this paper [3] recently, different techniques are available for data hiding. When to send some confidential data over insecure channel it is mandatory to embed data in some host or cover media. The advantage of this paper is the data hider compress the image to create sparse space to accommodate some additional data. Disadvantage is it is difficult to handle.

In this paper [4] this work proposes a novel Reversible Image Data Hiding (RIDH) scheme over encrypted domain. The information embed is achieve from side to side a public key modulation mechanism, in which access to the secret encryption key is not needed. Is able to perfectly reconstruct the original image as well as the embedded message. Need to, contain a relation to the carrier signal.

In this paper [5] the transmission of confidential data over the network requires more security. So, for improving security in data transmission, we can hide the data inside an encrypted image. Reversible Data Hiding. The original image can be recovered lossless.

III METHODOLOGY

3.1 ALGORITHM RSA:

Public-key cryptography moreover recognized as asymmetric cryptography, use two dissimilar but mathematically coupled key, one public and one private. The public key can be share with each one, whereas the private key must be reserved secret.

Security of RSA

The security of RSA depend on the computational difficulty of factoring large integers. As computing power increases and more efficient factoring algorithms are locate, the ability to factor larger and larger numbers also increases. Encryption power is frankly fixed to key in amount, and replication key length deliver an exponential increase in strength, although it does impair performance. RSA keys are commonly 1024- or 2048-bits long, but experts believe that 1024-bit keys could be broken in the near future, which is why government and industry are moving to a minimum key length of 2048-bits.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers x and y.
2. Compute $n = XY$. n is used as the modulus for both the public and private keys. Its length, normally expressed in bits, is the key length.
3. Compute the so called "Euler's totient function"φ (n) like this φ (n) = φ (x) φ (y) = (x − 1) (y − 1). It basically indicates the number of occurrences for which a specified integer k is coprime (that is, n and k only common divisor is 1) with n less than or equal to n.
4. Choose an integer e such that $1 < e <$ φ (n) and gcd (e, φ (n)) = 1; i.e., e and φ(n) are coprime.
    - e is released as the public key exponent.
5. Determine e (mod φ(n)) as an inverse of an integer d
    - $d^{-1} \equiv$e(mod φ(n))

- This is additional obviously confirmed as solve for d given $de \equiv 1$ (mod φ(n))
- This is often computed using the extended Euclidean algorithm.
- d is kept as the private key exponent.
- The computation of d^1.

Propose a information hiding and extraction procedure for high resolution VI (Video Interleave) videos. Even though VI video be big in size but it can be transmit since resource to object over network after giving out the source video by using these Data Hiding and Extraction procedure securely. There are two dissimilar actions which are used here at the sender ending and receiver ending respectively. The events be use here as the key of information Hiding and Extraction.

ADVANTAGES

- Attackers cannot find the original data.
- It is not easily cracked.
- To increase the Security.
- To increase the size of stored data.
- Hide more than one bit.

IV EXPERIMENT AND RESULTS

The proposed method has been implemented using. .NET Technology. achievement is the phase of the development when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The achievement phase involve alert preparation, analysis of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of Changeover methods. For more security provides by **RSA.** The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is currently one of the favorite public key encryption methods. Here is the algorithm:

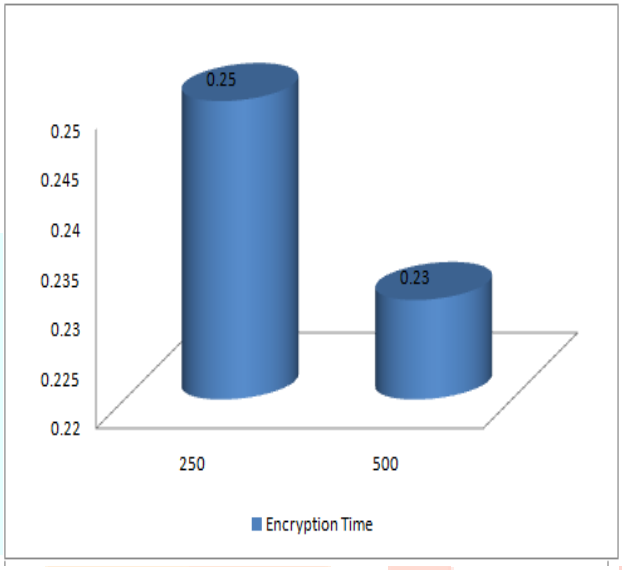
4.1 ENCRYPTION TIME

The amount of main time required to execute the encryption algorithm, where the input amount of data depends on the user input is known as the encryption time. The encryption time is also termed as the time complexity of algorithm. The Chart 1 and the table 1 show the encryption time.

Table 4.1 Encryption Time Analysis Table

File Size (MB)	Encryption Time	Encryption /Byte
250	0.25	0.0000125
500	0.23	0.0000128

Fig: 4.1 Graphical Representation of the Encryption Time Analysis



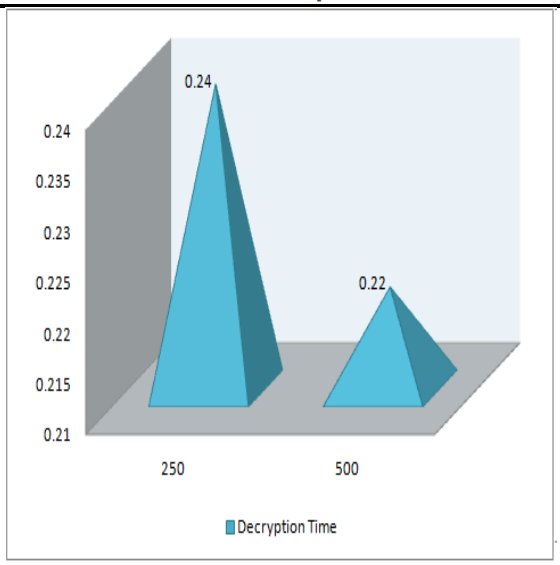
4.2 DECRYPTION TIME

For a cryptographic algorithm the amount of main time required, to recover the original text from cipher is explain as decryption time. That can also be termed as space complexity of decryption. The Chart 4.2 and table 4.2 shows amount of time consumed during data recovery. In the diagram X axis shows the different file size used for experimentation and Y axis reports amount of main time consumed.

Table 4.2 Decryption Time Analysis Table

File Size (MB)	Decryption Time	Decryption /Byte
250	0.24	0.0000135
500	0.22	0.0000126

Fig: 4.2 Graphical Representation of the Decryption Time Analysis



IMPLEMENTATION

Authentication

It consists of the username and the password fields. If these fields are valid then only it's possible to view this project. If these fields are invalid it's prompt out the error message like "Invalid String".

Embedding a message/file in a video file

This module is used to hide message in picture files. Video Location, Save File Location, Encryption Key are provided by the user to hide message in the save file location.

Retrieving the embedded message/file from the video file

This module is used to extract files. Downloaded images by the user are given as input in this text box**.** The key used to extract the file. This is a secret key. Receiver should know this key to retrieve message. This is the offset of the file where actually the picture file is resided.

Key Generation

Select p, q	p, q both prime, p≠q
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1) \times (q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

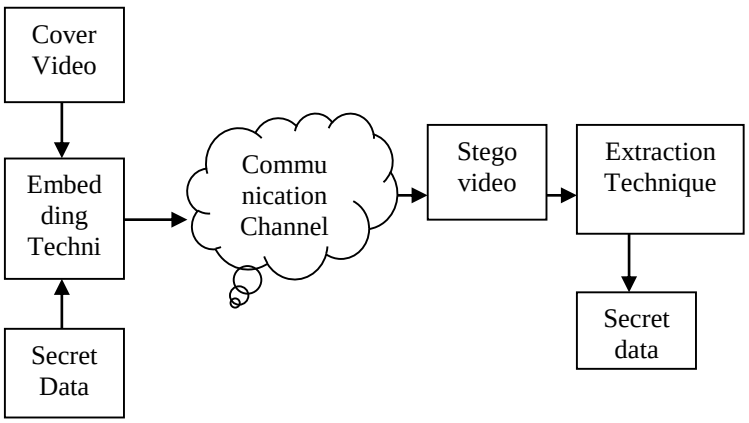


Fig. SYSTEM ARCHITECTURE

RESULT

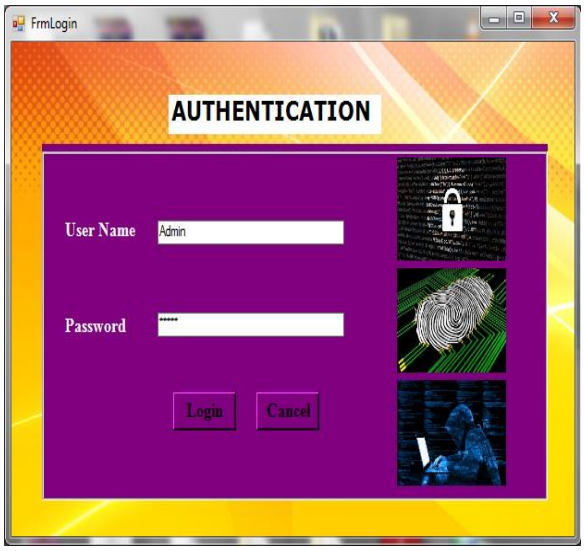


Fig 4.1.2 ADMIN LOGIN

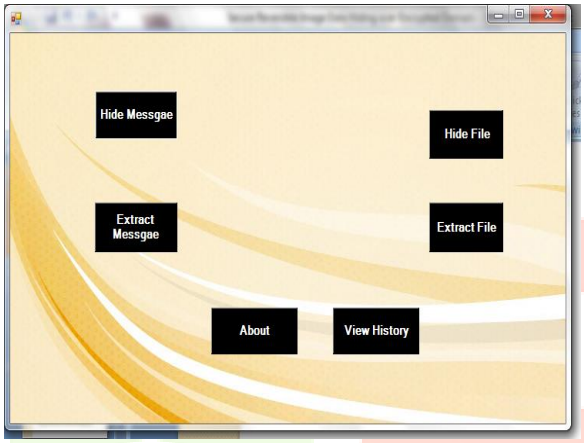


Fig 4.1.2 MAIN PAGE

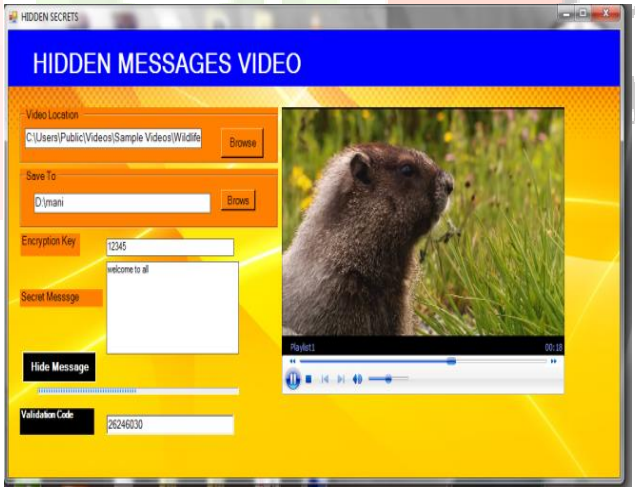


Fig 4.1.3 Message Encryption

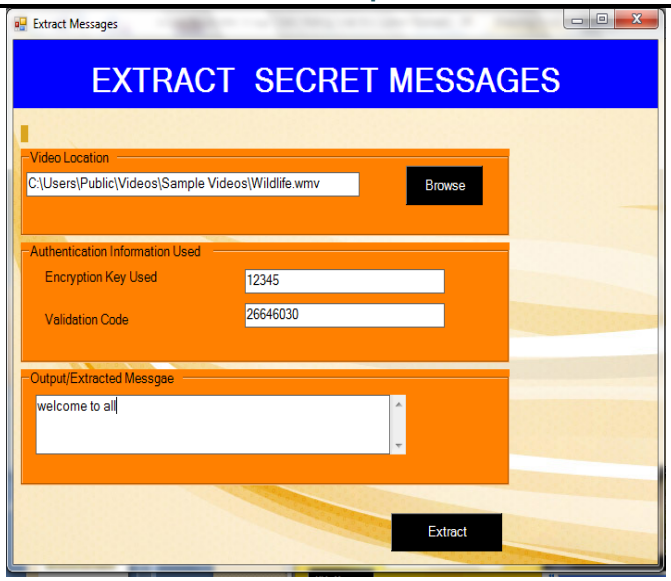


Fig 4.1.4 Message Decryption

IV. CONCLUSION

A secure video data hiding (VDH) scheme operated over the encrypted domain. A public key modulation mechanism, which allows us to embed the data via simple RSA algorithm, without the need of accessing the secret encryption key. To use a authoritative two-class technique classifier to differentiate encrypt and non-encrypt video patch enable us to both decode the surrounded letter and the original case signal perfectly.

REFERENCES

[1] Noise models in digital image processing Ajay Kumar Boyat1 and Brijendra Kumar Joshi2-2, April 2015.
[2] A survey on security issues: digital images Srinivas Koppu1, madhuviswanatham-18-06-2016.
[3] A Survey on Separable Reversible Data Hiding in Encrypted Image Ganesh Gunjal- 7, July 2015.
[4] Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation J. W. Zhang-2014.
[5] A Survey on Data Hiding Techniques in Encrypted Images- Minu Lalitha Madhavu- 1, January 2016.
[6] Alexandre H. Paqueta, Rabab K. Ward, Ioannis Pitas, Wavelet packets-Based digital watermarking for image Verification and authentication. Signal Processing.2003.
[7] T. Amornraksa, K. Janthawongwilai. Enhanced images watermarking based on amplitude modulation. Journal Image and Vision Computing.2006.
[8] Haohao song_, songyu yu, xiaokang yang, li song, Chen wang. Contourlet-Based
Image adaptive Watermarking. Signal processing: image communication. 2008.
[9] Han-Min Tsai, Long-WenChang. Secure reversible visible mage watermarking with authentication. J Signal Processing: Image Communication.2010.
[10] YounhoLee, Heeyoul Kim, Yongsu Park. A new data hiding scheme for binary image authentication with small image distortion.J Information Sciences.2009