Effective Key Generation Of Multimedia Applications

Mohammad Shoeb, Vishal Kumar Gupta

Abstract-The project entitled Effective key Generation for Multimedia Application is the application developed to embed an video file in another video signal. It is concerned with embedding information in an innocuous cover Speech in a secure and robust manner. This system makes the Files more secure by using the concepts Steganography and Cryptography, Steganography, poor cousin of Cryptography is the art of hiding messages inside other messages such that the very existence of the message is unknown to third party. The goal of cryptography is to make data unreadable by a third party, the goal of Steganography is to hide the data from a third party Through the use of advanced computer software, authors of images and software can place a hidden trademark in their product, allowing them to keep a check on piracy. This is commonly known as watermarking. Hiding serial numbers or a set of characters that distinguishes an object from a similar object is known as finger printing. Together, these two are intended to fight piracy. The latter is used to detect copyright violators and the former is used to prosecute them. But these are only examples of the much wider field of Steganography.The cover data should not be significantly degraded by the embedded data, and the embedded data should be as imperceptible as possible. The embedded data should be as immune as possible to modifications from intelligent attacks or anticipated manipulations. Thus it is necessary that the hidden message should be encrypted.

Index Terms: Steganography, Security, Encryption, Decryption, Private key Cryptosystem, Watermarking, GUI module

1 INTRODUCTION

Encryption of data plays a vital role in the real time environment to keep the data out of reach of unauthorized people, such that it is not altered and tampered and sending the in video format is most secured way to transfer the data through the network. The Video Stegnography is software, which tries to alter the originality of the file into some encrypted form and embed the file into an video file. The major task of the Video Stegnography is to provide the user the flexibility of passing the information implementing the encryption standards as per the specification and algorithms proposed and store the information in a form that is unreadable. The Application should have a reversal process as of which should be in a position to de embed the data file from video file and decrypt the data to its original format upon the proper request by the user. While the Encryption and Decryption is done the application should confirm the standards of authentication and authorization of the user.

The Entire application should strive to achieve a user friendly Graphical User Interface, which need to be in a self-learning mode for the end user. The System Should provide all the functional standards of proper navigation with in the environment, which makes it possible for the users to have a smooth flow while working under the environment. The Overall system should provide proper menu based navigation for easier navigation and operation. The Application should be designed in such a way that, as soon as it starts create a Buffer and associate this buffer to some homogeneous data environment, the application should ask the user for the Encryption Key details and should start its functionality upon the logistics that are provided with in this key. The key should be designed in such a way that it prevents the unauthorized persons from stealing the information at any point of time. This is some part of securing the data from third party people. And the other way of securing the data is using Steganography in which embedding the encrypted file in to a video file. If any one track that file they only see the video file not the data.

The application of De-embedding, Decryption should be a reverse process at the other end and should be translated only when the receiver of the data applies the proper reversal key. The Decryption process should have a log-based methodology that will take care of any errors that may be encountered while the system is under utilization and should record all those events, which are above the general standards of security.

This system basically uses the Tiny Encryption Algorithm to encrypt the passwords. This algorithm is a 64-bit block cipher with a variable length key. This algorithm has been used because it requires less memory. It uses only simple operations, therefore it is easy to implement.

2. Existing System

In the traditional architecture there existed only the server and the client. In most cases the server was only a data base server that can only offer data. Therefore majority of the business logic i.e., validations etc. had to be placed on the clients system. This makes maintenance expensive. Such clients are called as 'fat clients'. This also means that every client has to be trained as to how to use the application and even the security in the communication is also the factor to be considered. Since the actual processing of the data takes place on the remote client the data has to be transported over the network, which requires a secured format of the transfer method. How to conduct transactions is to be controlled by the client and advanced techniques implementing the cryptographic standards in the executing the data transfer transactions. Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. And also we have to consider the transfer the large amount of data through the network will give errors while transferring. Nevertheless, sensitive data transfer is to be carried out even if there is lack of an alternative. Network security in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange.

3. Proposed System

The proposed system should have the following features. The transactions should take place in a secured format between various clients in the network. It provides flexibility to the user to transfer the data through the network very easily. It should also identify the user and provide the communication according to the prescribed level of security with transfer of the file requested and run the required process at the server if necessary. In this system the data will be sending through the network as a video file. The user who received the file will do the operations like de embedding, and decryption in their level of hierarchy etc.

4. Literature Survey

Cryptography refers to the art of protecting transmitted information from unauthorized interception or tampering. The other side of the coin, cryptanalysis, is the art of breaking such secret ciphers and reading the information.

4.1 Mathematical Explanation

The first step is to choose a super increasing sequence of numbers of positive integers. A super increasing sequence is one where every number is greater than the sum of all proceeding numbers.

S= (s1,s2,s3,………,sn)

The second step is to convert all the characters of the message into binary. The binary sequence is represented by the variable b.

Third step is to choose two numbers: an integer „a‟ which is greater than the sum of all numbers in the sequence „s‟ and its co-prime „r‟. The sequence„s‟ and the numbers „a‟ and „r‟ collectively form the private key of the cryptosystem. All the elements of „s‟ are multiplied with the number „r‟ and the modulus of the multiple is taken by dividing with the number „a‟. i.e pi = r*si mod(a)

All the elements p1,p2,p3 ,……pn of the sequence p are multiplied with the corresponding elements of the binary sequence b. The numbers are then added to create the encrypted message Mi The sequence M = (M1, M2, M3,……, Mn) forms the public key of the cryptosystem.

4.2 RSA Cryptosystem

In 1978, Ronald L Rivest, A. Shamir and Leonard M. Adleman [2] proposed a method for realizing public key encryption as suggested by Deffie and Hellman [3]. RSA is a public key algorithm that is used for encryption, Signature and Key Agreement.. RSA typically uses the size of 1024 and 2048. The RSA standard is specified RFC 3447, RSA Cryptography Specifications Version 2.1 RSA cryptography system with public keys, based on modular exponentiation is considered as the most reliable cryptography system in the world. An overview of RSA is given below where a participant creates the public and private keys.

4.2.1 Parameter Generation

1) Select two large prime numbers p and q.

2) Find n=p*q, where n is the modulus that is made public. The length of n is considered as the RSA key length.
3) Choose a random number „e‟ as a public key in the range 0<e< (p-1)(q-1) such that gcd(e,(p-1)(q-1))=1
4) Find private key d such that (e*d) mod (p-1)(q-1))=1 Encryption Consider the device A that needs to send a message M to B securely
5) Let e be B‟s public key. Since e is public, A has access to it.
6) To encrypt the message M, represent the message as an integer in the range 0<M<n.
7) Cipher text C = (Me) mod n, where n is the modulus.

4.3 Decryption

8) Let C be the cipher text received from A.
9) Calculate Message M = Cd mod n, where d is B‟s private key and n is the modulus. It is easy to generate large prime numbers and multiply them but it is extremely difficult to factor the product. The RSA technique is costly, relatively slow and thereby limiting the throughput rate.

5. System Analysis

People for long time have tried to sort out the problems faced in the general digital communication system but as these problems exist even now, a secured and easy transfer system evolved and came to be known as the Encryption and Decryption of the data and converting the file to video format to be transferred using the cryptographic standards and Steganography. The advantages of this Effective key Generation for Multimedia Application are:

- High level Security
- Cost effective transfer

In this fast growing world where every individual free to access the information on the network and even the people are technically sound enough in hacking the information from the network for various reasons. The organizations have the process of information transfer in and out of their network at various levels, which need the process to be in a secured format for the organizational benefits.

If the organizations have the Effective key Generation for Multimedia Application System, then each employee can send the information to any other registered employee and thus can establish communication and perform the prescribed tasks in secured fashion. The video file that the employee sends reaches the destinations within no time in an video file format where the end user need to de embed the file, decrypt it and use for the purpose. The various branches of the organization can be connected to a single host server and then an employee of one branch can send files to the employee of another branch through the server but in a secured format.

6 Conclusion :

The entire project has been developed and deployed as per the requirements stated by the user, it is found to be bug free as per the testing standards that is implemented. Any specification-untraced errors will be concentrated in the coming versions, which are planned to be developed in near future. The system at present does not take care of lower level check constraints in accessing the file types in distributed environments, which is to be considered in the future up gradations.

As per the present status the project developed is well equipped to handle the Central file system of an organization in a server and provide access to the users with various privileges as prescribed by the higher authorities in the password file.

7 Reference.

[1] R.C. Merkle and M. Hellman, Hiding Information and Signatures in Trap Door Knapsacks, IEEE Trans. Inform. Theory, vol 24 1978,pp 525-530.
[2] R. L. Rivest, A Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the Association for Computing Machinery, vol 21, no.2, pp 120-126.
[3] W. Diffie and M. E. Hellman, New direction in cryptography, IEEE Transactions on Information Theory, vol. IT- 22 ,no. 6,pp.644-654.K. Elissa,

[4] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure Steganography model In Proceedings of International Conference on Advanced Computing and Communication Technologies (ICACCT-2008), Panipath , India 2008.

[5] G. Simmons, The prisoners problem and the subliminal channel, CRYPTO, 1983

[6] Souvik Bhattacharyya. and Gautam Sanyal. An Image Based Steganography Model for Promoting Global Cyber Security. In Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, India , 2009.

[7] K. Ahsan and D. Kundur, Practical Data hiding in TCP/IP, Proceedings of the workshop on Multimedia security at ACM Multimedia, 2002

[8] J.Silman, Steganography and Steganalysis: An Overview, SANS Institute, 2001

[9] Y.K. Lee and L.H. Chen, High capacity image steganographic model, Visual Image Signal Processing,147: 03, June 2000

[10] R. Krenn, Steganography and Steganalysis, www.krenn.nl/univ/cry/steg/article.pdf