International Journal of communication and computer Technologies, ISSN: 2278-9723

Available at http://www.ijccts.org

Key Hiding of Multimedia Applications in Multimedia File

Vishal Kumar Gupta, Mohammad Shoeb

Computer science & Engineering, Institute of Technology & Management.,

Received: 16-01-2013, **Revised:** 29-01-2013, **Accepted:** 26-03-2013, **Published online:** 19-05-2013

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.

Keywords **: Steganography, Security, Encryption, Decryption, Private key Cryptosystem, Watermarking, GUI module.**

I. INTRODUCTION

The inability of human users to remember strong cryptographic keys has been a factor limiting the security of systems for decades. History has proved that users can remember only short passwords.which was initially developed with the goal of utilizing keystroke timings in the generation of a strong key from a password. 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 within 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 anyone 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.

II. SYSTEM ANALYSIS

A. 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.

In the existing system we use Lotus approach which proposes the notion of hierarchy subgroup for scalable and secure multicast. In this method, a large communication group is divided into smaller subgroups. Each subgroup is treated almost like a separate multicast group and is managed by a trusted group security intermediary (GSI).GSI connect between the subgroups and share the subgroup key with each of their subgroup members. GSIs act as message relays and key translators between the subgroups by receiving the multicast messages from one subgroup, decrypting them and then re multicasting to the next subgroup after encrypting

A. 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.

In the proposed system we use an identity tree instead of key tree in our scheme. Each node in the identity tree is associated with an identity. The leaf node's identity is corresponding to the user's identity and the intermediate node's identity is generated by its children's identity. Hence, in an identity tree, an intermediate node represents set users in the sub tree rooted at this node.

III. LITERATURE SURVEY

The rapid penetration of increasingly sophisticated technologies into every facet of society is causing significant shifts in how, when, and where we work, how individuals, companies, and even nations understand and organize themselves, and how educational systems should be structured to prepare students effectively for life in the 21st century. School-aged children worldwide are growing up immersed in a media-rich, ubiquitous, "always connected" world. Concerns over the need to reform the educational system to effectively prepare students for a much more technology driven, interconnected and competitive "flat world" are being voiced by politicians, educators, parents, and others across the globe and security. Continuing to provide the security in secure key exchanging and key generation through the legal application system the challenges imposed by the rapid rate of technological change on society are significant, as the skills and knowledge imparted of key sharing no longer seen. 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.

IV. ALGORITHM EXPLANATION

The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm designed to minimize memory footprint and maximize speed. It is a Feistel type cipher that uses operations from mixed (orthogonal) algebraic groups. This research presents the cryptanalysis of the Tiny Encryption Algorithm. In this research we inspected the most common methods in the cryptanalysis of a block cipher algorithm. TEA seems to be highly resistant to differential cryptanalysis, and achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32-64 bit differences in the cipher text) after only six rounds. Time performance on a modern desktop computer or workstation is very impressive.

V. MATHEMATICAL EXPLANATION OF ALGORITHM

The Tiny Encryption Algorithm (TEA) was first published in 1994 by Roger Needham, and David Wheeler from Cambridge University of the United Kingdom. TEA was initially designed to be an extremely small algorithm when implemented in terms of the memory foot print required to store the algorithm. This was accomplished by making the basic operations very simple and weak; security is achieved by repeating these simple operations many times. As the basic operations are very simple TEA is also regarded as a very high speed encryption algorithm. These properties have made TEA a choice for both weak hardware or software encryption implementations in the past as TEA can be operated in all modes as specified by DES as outlined in the specification.

There are many notable fallbacks of TEA and it is considered broken. The first issue of note is that TEA uses "equivalent keys" thus weakening the effectiveness of its key length and requires only complexity O(2^32) using a related key attack to break. This is much less than the intended key brute force strength of 2^128. Two revisions of TEA have since been published including XTEA and XXTEA which boast enhanced security and the ability to support arbitrary block sizes making TEA obsolete as a secure cryptographic method.

The specification for TEA states a 128-bit key is to be divided into four 32-bit key words and the block size of each encryption is 64 bits, of which is to be divided into two 32-bit words. TEA utilizes a Feistel scheme for its encryption rounds in which 1 round of TEA includes 2 Feistel operations and a number of additions and bitwise XOR operations. The specification simply "suggests" that 32 TEA rounds be completed for each 64-bit block encrypted, all online resources appear to follow this suggestion. This means a full encryption of a block is simply 32 TEA rounds which involve 64 Fiestel rounds.

Input	Output
Plaintext	Cipher text
00000000 00000000	4e4e642a 43de3739

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.

VI. SYSTEM DESCRIPTION

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.

VII. CONCLUSION

The Proposed system is an efficient, authenticated, scalable key agreement for large and dynamic multicast systems, which is based on the bilinear map. New modules are in pipeline for to increase the compatibility of the project. Once these improvements have been done, the majority of the features that make an application an excellent one would be there and the usage would become wider. 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.

REFERENCES

[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] Y. Amir, Yakima, C. Nita-Rotary, J. L. Schultz, J. Stanton, and G.Tsudik, ”Secure group communication using robust contributory key agreement,” IEEE Trans, Parallel Distrib. Syst., vol: 15, no.5, pp, 468-480, May 2004.

[5] G. Ateniese, M. Steiner, and G. Tsudik, “Authenticated group key agreement protocols,”in Proc.5th Annu. Workshop on selected Areas in Cryptography Security (SAC’98), 1998, pp. 17-26.

[6] S.Blake-Wilson and A.Menezes, “Authenticated Diffie-Hellman Key agreement protocols,” in Proc. 5th Annu. Workshop on selected Areas in Cyrptography (SAC’98), 1998, vol. LNCS 950, pp. 275-286.

[7] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654,1976