STEGANOGRAPHY USING DYNAMIC KEY GENERATION

Priyanka Kumari, Aritra Pal, Parth Dixit
Under Guidance of Dr. A. Shanthini

SRM University, Kattankulathur

ABSTRACT

The communication processes today are prone to lot of sensitive information. So much that any diversion from security tend to destroy someone's hard earned money or to throw a whole nation into an economic turmoil. Cryptography provides a way to tackle this by making sure that the sensitive information remains in the hands of the intended user. However, cryptography is prone to cryptanalysis attacks. To reduce the risk, we have used a dynamic key theory. Because these dynamic keys are one-time symmetric cryptographic keys, they can significantly improve the security of cryptographic systems. Still, if we are to send a cryptic message in open, the unintended user may find ways to decrypt the message. So, we in this project are presenting a way of communicating via cryptic messages in the open and do this without any possibility of detection. The plain text is converted to a cipher text via a new dynamic key generation technique and then encoded into an image steganography model to hide the same information in an image.

The reason for doing this is to provide a dual protection layer of the message. The message is itself in an unintelligible format and encoded in an image. For a person to decipher the hidden message, he has to have a knowledge of the data being hidden inside the image as well as the decryption algorithm for the message to decipher. This decipherment will not be entertained by brute force attacks or key guessing, since the key as well as text for the encoding will be in different formats.

INTRODUCTION

One of the important reasons that attackers or intruders can be successful is because most of the information they obtain from a system is in a form that they can only read and comprehend. Intruders may expose the information in front of others, alter it to misrepresent an individual or organization, or utilize it to launch an attack. One of the best solution to this problem is hiding the information in a way that the intruder doesn't have any idea about the information. We use data hiding methods such as steganography and cryptography. Steganography is a method of hiding information in digital media. Unlike cryptography, Steganography is not about keeping others away from knowing the hidden data but it is to keep others away from thinking that the data even exists.

Steganography becomes much more important as people join the cyberspace revolution. Steganography is the method of hiding the information in different ways which prevents the detection of hidden information. It includes an array of secret communication techniques that hide the information from being seen or discovered by the intruders.

Due to amendment in ICT, most of the information is kept in electronic format. Consequently, the security of information has become an important issue. Besides steganography, cryptography can also be employed to secure the information. In cryptography, the message or an encrypted message is implanted in a digital host before passing it across the network, thus the existence of the message remains unknown. Besides hiding data for the purpose of confidentiality, this approach of hiding information can be expanded to copyright the security for digital media: audio, video and images.

The increasing possibilities of modern communication process needs special means of protection especially on computer network. The network security is becoming more and more important as the rate of information being exchanged over the internet increases. Therefore, the data confidentiality and data integrity are required to be kept safe against unauthorized access and use. This has resulted in an explosive increase in the field of information hiding

Information hiding is a growing research area, which encompasses the applications such as copyright security for digital media, watermarking, fingerprinting, and steganography.

In the watermarking applications, the encrypted message contains information such as identification of owner and a digital time stamp, which is generally applied for protection of copyright .

In fingerprint, the owner of the data set imparts a serial number or key that uniquely identifies the user of the data set. This adds to copyright the data to make it possible to trace unauthorized user of the data back to the user.

Steganography hides the secret message within the data set of the host and makes its presence imperceptible and is to be reliably communicated to a end user. The host data set is corrupted on purpose, but in a covert way, designed to be invisible to any kind of information analysis.

LITERATURE REVIEW

Various algorithms have been developed and introduced in the past years for the process of encryption. Some of the algorithms worked very conveniently, but they do have some overheads relating to them. There has been a inexplicable amendment in the field of cryptography, since the concept of internet security has come into play, the old algorithms have still retain their value in various applications and so before discussing the current research trends, it is important to have a clear knowledge on the ancient popular symmetric key algorithms.

Horst Feistel developed Data Encryption Standard (DES), a symmetric key algorithm which

is used to encrypt block of data which is based upon Balanced Feistel network. The DES algorithm uses 16 different iterations on the data and was designed such as to operate on different modes. The key size of DES is 56 bits, which can be broken down by using bruit-force techniques [4].

To reinforce the conduct of DES, Triple DES was introduced in 1998. Triple DES has a key size of 64 bits. The data is encrypted using three distinct keys. Each data block is encrypted using different keys of size 56 bits. Both sender and receiver have to follow a complex steps to attain the encryption and decryption process in 3 levels. Also the complexity of algorithm is increased by large key size. Moreover the keys used in this algorithm are of fixed size and are static. Thus it is easy for the attacker has always to find the key by applying bruit-force techniques [5].

Rijmen V, Daemen J (1998) developed The Advanced Encryption Standard (AES). In AES algorithm block size is of 128 bits which is fixed throughout the process, and key lengths are varied. It can be of 128-bits, 192-bits or 256-bits [6].

Kim et al. (2005) have proposed an algorithm on symmetric key cryptography for a video file. The authors developed a protection theme for MPEG-4 video file format. During this protection theme, small segments of each Video Object Plane in an every MPEG-4 video file can be encrypted with any of the symmetric key cryptographic algorithm. developed So people who don't have the permission to receive and/or have not paid to utilize the contents of the file wouldn't be able to read and view them. This scheme is applied to all kinds of MPEG-4 Video Object Plane types,i.e., I-, P- and B severally [7].

Debnath Bhattacharya et al. (2009) have proposed an approach to steganography to ensure data security [3]. In this algorithm, they used a combination of cryptography, steganography and an extra layer of security to encrypt text messages. This algorithm used two public keys and one primary key to encrypt data. This concept of layers enhances computation time thrice to encrypt/decrypt the text message. Moreover this security algorithm works only for the text messages and not for other formats [1].

V.S.Shankar Sriram et al. (2010) proposed an interesting Block Cipher Multiple Key Symmetric Encryption (BCMKSE) algorithm to dwindle the computational and performance time as well as message overhead [8]. As this way is based on symmetric key, two private keys which are NOBS (no of bits) and the Key K are computed and shared among receiver sender and receiver by some other modes. The key is computed by various components like generating MINi (i.e., client node related), MINs (i.e., server related), SRMPNi (which is based on screen resolution and mouse position) and Ti (which is a time component). In the same manner NOB is obtained by applying XOR, addition functions on these components. It is very tough for eavesdropper to hack the private keys. This symmetric key approach is secure enough, but this approach has a lot of overhead to calculate the values of Key K and NOB which are fixed values and can be assumed as well to diminish computational overhead. Also the key is composed of a combination of server and client related information, which can be easily approached and

utilized by an attacker to bring out the key and the number of permutations for NOB were less. Any intellectual attacker can find the key with little overhead of applying permutations. Moreover, this technique has an extra overhead of using MD5 to ensure the integrity of the message [2].

Aditee Gautam et al. (2011) introduced a new technique using block (block of data) based transformation which is used for encryption of the image. Here the image is modified into other image before the process of encryption is over. Blowfish algorithm is used for this transformation process [1]. Blowfish has a 64-bit block size and a variable length of key varies from 32 bits up to 448 bits. It is based upon 16 rounds. There are various key dependent permutations, variable keys used on data at each round with XOR, addition operations. Blowfish is fast block based algorithm, when the same key is used. But computation time enhances with changing keys. Every new key requires pre-processing equivalent to encrypting text, which is very slow when compared to other algorithms. Secondly, if there is lack of simultaneity between two parties then it will not be able to use the same key for encryption and decryption process [8].

Mazloom et al. (2011) has introduced a new symmetric key cryptography for images. This algorithm use secret key of size 128 bits . This algorithm used confusingly–diffusion architecture which uses the concept of chaotic (2 Dimensional) Standard map and (1 Dimensional) Logistic map. This algorithm is especially designed for the color images, which are 3D arrays of RGB data stream. The introductory conditions and parameters related to system of the chaotic maps compose the secret key of the algorithm. This algorithm used some properties of mixing horizontally and vertically adjacent pixels using a Logistic map, for getting better security and complexity [9].

Niraj et al. (2013) conferred various issues in symmetric key based cryptographic algorithm used for videos and images. Author has featured that when the ciphered text is generated, it is decrypted into normal plain text without any loss, whereas, the encrypted images may not be decrypted to actual images without loss. Also, conventional crypto systems take time to encrypt/decrypt the images because the size of the image is usually larger than the text message. The author has also conferred that Video data cannot be directly encrypted or decrypted. First video data is transformed into a number of image frames and then conventional cryptography algorithms like DES, AES and RSA are applied on every individual image frames. These algorithms are not applicable for video as well as color images. Although some of the lossless encryption systems use the symmetric properties of the orthogonal transform to evaluate the inverse of the orthogonal matrix in the decryption process to speed up the operations and reduce the cost of performance but they also have impose additional overhead of other transforms, Key-Gen algorithms and XOR operations that has increased the encryption time severely [10]. The authors have also focused on the challenges in multimedia cryptography techniques. The author conferred various techniques of image cryptography and video cryptography including [9] and [7]. These techniques use complex steps and chaotic confusions and diffusions for better

security. As these techniques are based on conventional text based encryption algorithms like DES, AES, and RSA, therefore it may be possible that the decrypted image may lose some of the data.

For all the other above mentioned algorithms, two common problems are there. First is the much computation is required for different iterations. Second is the unique key size. The key is static. So, using a single key for long period of time doesn't entitle the message secrecy. Along with this, these techniques encrypt the message to a satisfactory level, therefore the cipher text can be cracked by using some complex permutation algorithm.

Multi-Layer Data Security algorithms combining Cryptography and steganography are used to enhance the level of security, but it also tend to improve the response time and hence increasing the time/space complexity, which is not acceptable for large volumes of data.

ALGORITHM AND WORKING OF PROPOSED APPROACH

The algorithm works on the fact that every time the message is encrypted, it gives a different cryptic message. This is done by including the date and time of the system. Since the date and time of the system will be unique every minute, there is no possibility that the encoded message can be found out by any means of the brute force attack. The key of the message to be decoded from is sent along with the code with the help of a separator. This separator will be in the form of a number so that no one other than the machine can understand that this will separate the encoded message and the key. Suppose that this is compromised, still, the key sent will also be encrypted so that the plausible understand ability of the decoding process is ruled out.

The method for encryption is by character wise encryption of the whole message. The message is broken down to 8 binary bits of character wise asci values. This value is xored with the addition of digits of date and time. Now, this bit wise xored product is added with the original bit wise value of the message. For example; A is 65 in asci. After adding the date and time it may become 97. Now we break the 65 in binary 8 bit to a further 4 bit. This is added simultaneously to the date-time added bit i.e. 97. All this is done in binary as a bitwise encryption system and the resultant array of the encoded bitwise characters are our encrypted message. Now, we add a separator to the encrypted message. Example : 34. We should choose this separator such that it should be less than the least asci amount of an alphabet. Here it is 65 for A. The key is then made by addition of character wise bit of the message with the addition of the whole encrypted message. This character wise addition makes up a key that can be used to decode the message by simply subtracting the key value with the encrypted message value.

After encryption, we send the message to a steganographic module which encrypts the encrypted message in an image. This message is stored in a text file that is encoded in the least significant bit of the original image. The message is then sent over to the receiver who can decode the image first and then apply the decryption algorithm to get the original message.

WORKING

Algorithm At Senders End

1. Sender enters a text message which is denoted by *m* ..
2. *ASCII value pattern of characters* present in the text message (i.e. *plain text*) is observed.
3. From this ASCII value pattern of the plain text a string of numbers is generated. This string of numbers is called *DYNAMIC KEY (D_yK).*
4. The original message is encrypted with the help of generated Dynamic Key. This *ENCRYPTED MESSAGE* is denoted by E_m
5. The *ENCRYPTED DYNAMIC KEY* (i.e , *EDyK*) is generated , using the following formula

$ED_yK = D_yK + X$, where X is the sum of digits present in the ASCII values

of the characters in the encrypted message (E_m).

6. Now the *ENCRYPTED MESSAGE* (E_m) and *ENCRYPTED DYNAMIC KEY* (EDyK) is sent to the receiver.

ENCRYPTION PROCEDURE

1. To generate the DYNAMIC KEY (D_yK_i) for each line of the plain text date and time will be concatenated with each line , where i denotes the line number of the plain text.
$D_yK=[D_yK_1D_yK_2D_yK_3\ldots\ldots\ldots\ldots\ldots D_yK_i]$, where i denotes the line number present in the text message.
2. ASCII value of the character of the line of the original text will converted from decimal to 8 bit binary. It will be separated into two parts, each consisting of 4 bit: C_iPLB, C_iPRB.

Then in the function module following steps will be done:

a) With each ASCII value of each character of a line (*i.e.*, C_iD_yK) add sum of digits of the date and time to generate C_i 'D_yK

b) To generate XC_iPRB we will do *XOR* operation between C_i "D_yK and C_iPRB.

3. To generate CH_iCRB we will do XOR operation between C_iPLB and XC_iPRB**.** It is 8 bit **.**

4.To make C_iPRB 8 bit adds extra 4 zeros in front of the C_iPRB. Now it is denoted by CH_iPLB.

5.To make the final cipher for each character concatenate CH_iPRB and CH_iCRB. So, for each 8 bit character here two 8 bit characters will be generated.

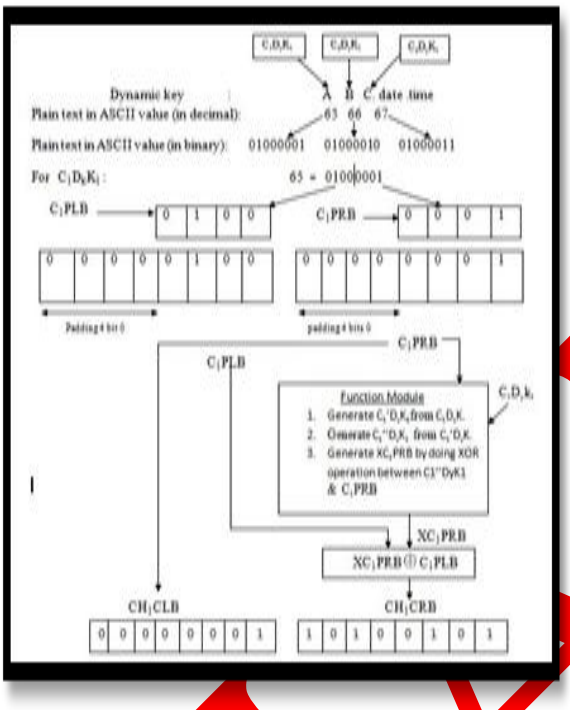
6.Now, sum of digit of ASCII value of each character of the cipher text of that line is calculated.

7.To generate *ENCRYPTED DYNAMIC KEY* add this sum of digit with *each ASCII value of each*

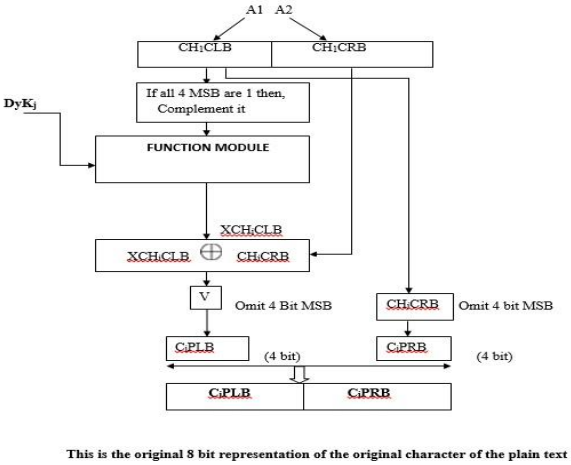
character of the plain text.

8. To generate the *FINAL CIPHER* of each line concatenate *CIPHER TEXT* , *EDyK* , *DATE &TIME*. Put a *separator (@)* between these *three* to distinguish one from the other.

9. To generate the final cipher for the whole plain text do the above mentioned steps for each line present in the plain text.



DECRYPTION PROCEDURE



This is the original 8 bit representation of the original character of the plain text

REFERENCES

1. Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, "Text Steganography: A Novel Approach", in International Journal of Advanced Science and Technology, Vol 3, Feb 2009.

2. V.S.Shankar Sriram, Abhishek Kumar Maurya, G.Sahoo, "A Novel Multiple Key Block Ciphering Mechanism with Reduced Computational Overhead", in International Journal of Computer Applications, Vol.1 (No.17):25–30, February 2010.

3. Guanrong Chen, Yaobin Mao and Charles K. Chui "A symmetric image encryption scheme based on 3D chaotic cat maps", in Elsevier Chaos, Solitons and Fractals 21 (2004) 749–761.

4. Federal Information Processing Standards Publication 46-3, "Data Encryption Standard (DES)", U.S. DoC/NIST, October 25,1999

5. American National Standard for Financial Services 1998, "Triple Data Encryption Algorithm Modes of Operation", American Bankers Association, Washington, D.C. X9.52- July 29, 1998.

6. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography algorithms simulation based performance analysis", in International Journal of Emerging technology and Advanced Engineering, Volume 1, Issue 2,December (2011).

7. Gunhee Kim; Dongkyoo Shin; Dongil Shin, "Intellectual property management on MPEG-4 video for hand-held device and mobile video streaming service", Consumer Electronics, IEEE Transactions on , vol.51, no.1, pp.139,143, Feb. 2005.

8. Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta "A New Image Encryption Approach Using Block Based Transformation Algorithm", international Journal of advanced engineering sciences and technologies Vol No. 8, Issue No. 1, 090 – 096, 2011.

9. Mazloom, S.; Eftekhari-Moghadam, A.M., "Color image cryptosystem using chaotic maps", Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP), 2011 IEEE Symposium on , vol., no., pp.142,147, 11-15 April 2011.

10. Niraj Kumar, Prof. Sanjay Agrawal, "Issues and Challenges in Symmetric Key based Cryptographic Algorithm for Videos and Images", in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

11. Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices", in International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009.

12. Pranam Paul, Saurabh Dutta, A K Bhattacharjee, "An Approach to ensure Security through Bit-level Encryption with Possible Lossless Compression", in International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008.

13. Gajendra Singh Chandel, Ravindra Gupta, Swati Jain, "Proposed Model of Dynamic encryption using Steganography" in International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 9, September 2012.

14. Nidhi Singhal, J.P.S.Raina, "Comparative Analysis of AES and RC4Algorithms for Better Utilization", in International Journal of Computer Trends and Technology, July to Aug Issue 2011.

15. D.S. Abdul Elminaam, H.M. Abdul Kader, M.M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithm", in Communications of the IBIMA, Volume 8, 2009 ISSN: 1943-7765.