European Journal of Academic Essays 1(2): 56-60, 2014
ISSN: 2183-1904
www.euroessays.org

Enormous Symmetric Cryptography Algorithm Using Image and Double Reflecting Data Perturbation Method

Balajee Maram[1], DrChalla Narasimham[2]

[1]P.hD(CS) part-time Scholar from Bharathiar University, Coimbatore

Sr. Asst. Prof., Dept of IT, G M R Institute of Technology, Rajam,

Andhra Pradesh - 532 127, India.*balajee.m@gmrit.org*

[2]Professor &HOD,Dept. of CSE, S R Engineering College, Warangal. *narasimham_c@yahoo.com*

Abstract: Information Security plays a vital in Data Communication in Intra-Organization and Inter-Organization. Till now so many algorithms have been introduced for providing Security to Data. Most of the algorithms are belongs to Cryptography. In Data Communication, the Data is encrypted using Private-Key/Public-Key. Then the encrypted data (Cipher) will be decrypted in Receiver-Side. For Data hiding, the Steganography techniques are very useful. In Steganography, Images are very important for carrying data. But this research paper proposes an enormous algorithm for Cryptography using Images. In the proposed algorithm, Double-reflecting Data-Perturbation method plays a vital for Encryption and Decryption. The proposed paper using Cryptography algorithm and shuffling data is converted into a Image. From Receiver-side, the Image is converted into ASCII and then data.

Keywords: Image, encryption, decryption, cryptography, double reflecting data perturbation method

1. Introduction

In every cryptographic algorithm, there is a need to either shared secret-key or private/public key pair. The strength of the encryption is based on the length of the key. When the length of the key is very small then it is very easy to crack the key as well as decrypt the data. In symmetric and asymmetric cryptography, the required keys should be shared in symmetric cryptography and the public key should be published in asymmetric cryptography techniques. Before data communication, the data will be converted into ASCII and divided into 24-bit chunks. All ASCII bits will be converted into Image.[1]

This paper proposes a new technique for encoding and decoding for data communication. Here we are trying to apply DRDP technique. In proposed encryption technique, each and every character has been calculated based on DRDP method only. Each and every bit is inserted into an Image. This proposed algorithm has been checked and verified in PYTHON language successfully. [1]

This proposed algorithm has been checked theoretically and practically.

Interpersonal communication is the methodfor exchanging information, ideas, thoughts and feelings through verbal and non-verbal massages. It is usually involves person to person interaction in which both the spoken and body language are used to communicate. Interpersonal communication is not just about what is actually said, but how it is said and the non-verbal messages sent through tone of voice, facial expression, gestures and body languages.

There are a variety of verbal and non-verbal forms of communication. These include body language, eye contact, sign language, communication etc. Other examples are media content such as pictures, graphics, sound, and writing. The Convention on the Rights of Persons with Disabilities also defines the communication to include the display of text, Braille, tactile communication, large print, accessible multimedia, as well as written and plain language, human-reader, augmentative and alternative modes, means and

Corresponding Author: Balajee Maram, Email: balajee.m@gmrit.org

formats of communication, including accessible information and communication technology.[4] Feedback is a critical component of effective communication. [2]

Data Communication is the process for conveying the information by the exchange of information, messages, feelings, thoughts etc. Like this, two persons can exchange their needs, desires, perceptions and knowledge. This is called Data Communication.

In Data Communication, there is a need of a sender, a recipient and a message. Here the presence of Recipient is optional i.e present or absent. Here the intention of the sender to sends data to the recipient. If the recipient is in online, then he will receive the message instantly. Otherwise the message will be stored in Message-Queue/Inbox. The Communication is called successful when both the persons exchange their information successfully[3].

Communicating with others involves three primary steps:

- Thought: First, information exists in the mind of the sender. This can be a concept, idea, information, or feelings.
- Encoding/Encryption: A message is sent to a recipient in words or other symbols.
- Decoding/Decryption: When the recipient translates the words, symbols or cipher into the information that a person can understand.

But in Secure Data Communication, there is a need to apply Cryptographic algorithms. But all algorithms are based on either private-key or public-key.

The proposed algorithm explains us how to send data with safe using Images and private-key. The procedure will be explained in the following Sections.

2.Existing System

2.1 CRYPTOGRAPY

Cryptography is the study and practice of encoding data using transformation techniques so that it can only be decoded by specific users. In simpler words, it is a theory of secret writing. Cryptography is the systems involving two kinds of security problems: privacy and authentication. A privacy system prevents the extraction information by unauthorized parties from messages transmitted over a public channel, thus assuring the sender of a message that it is being read only by the intended recipient.

Types of Cryptography

There are three main types of cryptography:

- Secret key cryptography
- Public key cryptography
- Hash function

Secret key cryptography – In this method, the data is encrypted and decrypted using a "shared secret" key. This type of encryption scheme is also known as symmetric key encryption. Here there is a need to share one common key which is known as "Secret-Key".

Public key cryptography – In this method, there is a need of two keys. The first key is known as "Public-Key" and the Second key is known as "Secret-Key". The plain text is encrypted with private-key of sender (or public-key of receiver). In receiver side, the cipher text is decrypted with public-key of sender (or private-key of receiver). Here, it is not necessary for the sending and receiving users to share the common secret. Here the recipient should distribute his own public-key.

Hash functions - Hash functions are one-way cryptographic schemes. Here, the plain text is being processed by the hash techniques and the output is the hash-value of the original text. From this hash-value, it is impossible to calculate the original information.

2.2. Double-Reflecting Data Perturbation Method

The Double-Reflecting Data Perturbation Method denoted by DRDP reverberates the original data by x-axis and y-axis to achieve the perturbed data for some confidential attribute. In this method, the randomization function plays a very crucial rule, and if the function is not properly chosen it May degrade the clustering quality. The distortion operation performed to the confidential attribute is given by

$$op_j = \rho_{Aj} + (\rho_{Aj - aj) = 2} \rho_{Aj - aj.}$$

Where Aj ($1 \leq j \leq n$) is a confidential attribute and a j ($1 \leq j \leq n$) is an instance of Aj. ρ_{Aj} is defined by the following formula

$$\rho_{Aj} = |(\max Aj + \min Aj)/2|$$

Where max Aj and min Aj are respectively the maximum value and minimum value of attribute Aj. The 'student' relational

database before and after applying DRDP is shown in the following Table:[4,5,6]

Table 1: Example on Double-Reflecting Data Perturbation Method

S.No	RollNo	Name	Marks	Distored Marks
1	101	Raj	78	92
2	102	Ravi	89	81
3	103	Rohan	92	78
4	104	Rani	82	88
5	105	Rahul	80	90

2.3 Definition of Image

An Image is a visual representation. In Digital Communication, an Image is a picture which is in digital form. The Image can be represented in the form of Vector Graphics. Below is an example of a computer generated image which is generated by using a computer software program.

Figure 1: Scenery

Image and Pixels

Pictures are made up of thousands of tiny dots, each of a single color. But in Digital Communication, they are called pixels.

The word 'pixel' stands for 'picture element'. Different Pixels representing different colours and shades very much like in reality.

A digital image is an array of pixels. A pixel is a set of 3 values indicating variations of red, green, and blue at a particular location on a grid of pixels.

Format of IMAGE

A digital image is nothing but an array of pixel values. There are different types of formats are available for storing an image in a file. The examples are .BMP, .JPEP, .PNG etc. A typical image file will have data as shown below:

111 114 118 119 118 105 85 71 73 72 66 69 80 89 92 90 92 93 82 78 92 92 95 100 04 107 108 109 109 112 108 100 92 84 73 60 50 50 54 54 46 39 42 57 72 86 87 90 94 99 105 109 112 115 113 108 101 92 87 89 93 100 102 91 76 68 55 48 56 72 76 76 66 54 53 67 81 94 78 56 42 48 68 85 92 96 97 104 114 115 100 79 64 60 61 66 77 84 78 60 45 49 42 50 72 83 71 55 49 42 41 39 40 43 43 35 24 45 49 54 57 58 58 110 114 122 124 121 97 72 53 52 53 49 52 62

Here each pixel is having 3 values with range from 0 to 255. The size of each value is 8-bits. Here 255 indicatesa white pixel and 0 indicates a black pixel. There are a total of (width * height) values. The pixels are stored in 2D array, starting at the top-left corner of the image, and left to right. [7]

3. Proposed System

3.1 ENCRYPTION

1. Share the Secret-Key between sender and receiver
2. Take the file which going to encrypt
3. According toASCII values of Secret-Key, characters will be shuffled in the text file using Double-reflecting Data Perturbation Method.
4. Each character will be converted into ASCII form.
5. Divide all the bits into 3-character chunks.
6. Each chunk of 3-character is converted into a single PIXEL
7. If the last 3-character chunk is having less than 3-characters, then ASCII value 255's will be added.
8. Now all the pixels are combined and formed as an IMAGE.

3.2 Decryption

1. In Receiver side, the received IMAGE will be converted into array of pixels
2. Each pixel will be converted into 3-character chunks.
3. Now each ASCII value is converted into characters.
4. The characters will be reshuffled based on the ASCII value of shared Secret-Key using Double-reflecting Data Perturbation Method.
5. Now the receiver will get the actual data.

4. Illustration

4.1 Encryption

1. Let us take the shared Secret-Key is "IMAGEPIXELS"
2. The file which is going to encrypt is "testdata.txt"

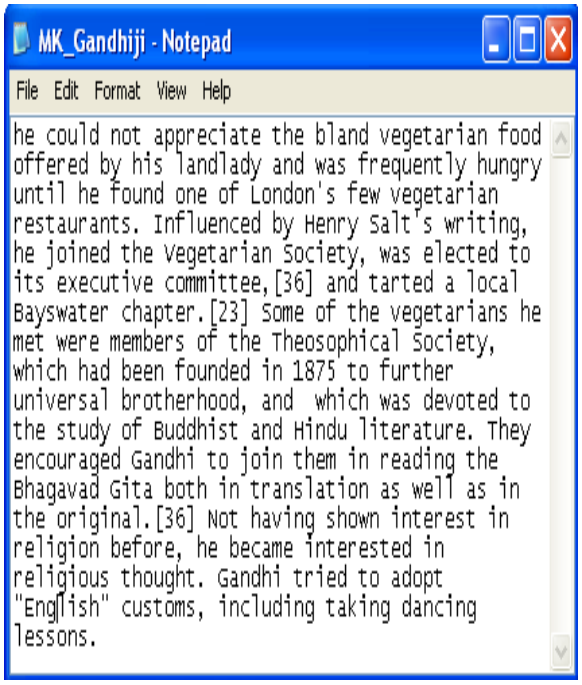

Figure2: Contents of Input text

3. According to ASCII values of Secret-Key, characters will be shuffled in the text file "testdata.txt". From the shared Secret-Key "IMAGEPIXELS", the ASCII value of 'I' is 73. So the first 73 characters in the text file "testdata.txt" will be shuffled. The ASCII value of next character 'M' is 77. The next 77 characters in the text file "testdata.txt" will be shuffled using Double-reflecting Data Perturbation Method. And So on.
   After shuffling, the above data will be like the following:

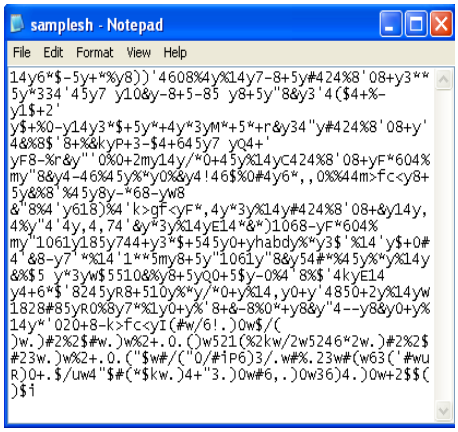

Figure3: Data – After Shuffling

4. After shuffling all the characters in the text file "testdata.txt", each character will be converted into ASCII form. The ASCII form is in the following way:

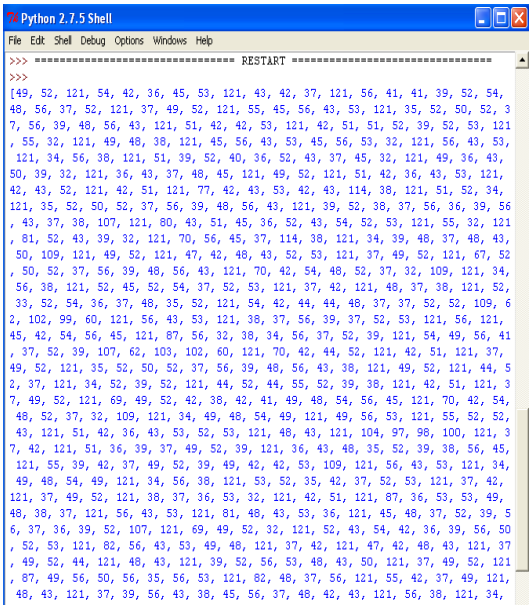

Figure4: Values of all pixels in IMAGE

5. Now 3-character chunks will be converted into a pixel. The output(IMAGE) is in the following way:

4.2 Decryption

1. Now the receiver will receive the following IMAGE.

2. This IMAGE will be converted into array of pixels except the last few black pixels. Because some values (255) have been added at the time of encryption if necessary.
3. Now each pixel is converted into a set of 3-ASCII values.
4. According to shared Private-Key, all the characters will be shuffled using DOUBLE REFLECTING DATA-PERTURBATION method.
5. Now the receiver will get the actual data.

5. Security Level

In 1st phase of proposed method, all the characters in the sentence are converted into UNICODE. Now those characters are shuffled according to their UNICODE value based on Double Reflecting Data Perturbation Method. The privacy of data is measured by the variance between the actual and the perturbed values which is given by the following formula:

$$A=\frac{VAR(A-A')}{VAR(A)}$$

It has been analyzed that the privacy or the security level of the confidential data is improved a lot by the proposed method for Encryption and Decryption [4,7].

6.PERFORMANCE ANALYSIS

The CONFIGURATION of the Computer System where this proposed algorithm has been executed:

Processor: Intel Core 2 Duo E7500@2.93GHz

RAM: 2 GB

Operating System: MS Windows XP

Hard-Disk: 500 GB

Table 2: List of sizes of Input and Output files with Encryption-Time, Decryption-Time

S. No	*File Name*	*Size of Input File*	*Size of Output File*	*Encryption Time*	*Decryption Time*
1	testdata1.txt	802 bytes	743 bytes	1 Sec	1 Sec
2	testdata2.txt	12.5 KB	2.27 KB	2 Sec	2 Sec
3	testdata3.txt	1.66 MB	193 KB	6 Sec	6 Sec
4	testdata4.txt	8.34 MB	961 KB	32 Sec	32 Sec
5	testdata5.txt	58.4 MB	6.6 MB	3 Min 28 Sec	3 Min 28 Sec

7. Conclusion

Till now many cryptographic algorithms have been observed. Every algorithm is simply based on text, private-Key, public-Key etc. But this proposed cryptographic algorithm is based on private-key, image and Double-reflecting Data-Perturbation Method. The Data-Perturbation Method is for shuffling the characters in the given text file. When we observe the Performance Analysis, always the size of the output file is less than the size of the input file. But the Encryption-Time and Decryption-Time are same. In this proposed algorithm, the security is based the size of the shared "Secret-Key". When the key size is more than security is more. But this proposed cryptographic algorithm has one limitation is that it encrypts text data only (Not working for Images).

References

[1]. Balajee Maram, DrChalla Narasimham, "A Cognitive Cryptographic approach using DRDP Method", European Journal of Academic Essays (EJAE), Vol: 1 (1), pp: 11-16, Jan' 2014.

[2].http://www.skillsyouneed.com/ips/interpersonal-communication.html

[3] http://en.wikipedia.org/wiki/Communication

[4].BALAJEE MARAM, Dr CHALLA NARASIMHAM, "Double Reflecting Data Perturbation Methodfor Information Security", OJCST, Dec' 2012, Vol:5, No.2, Pgs: 283-288

[5]. Wang Jing, Wang Xiaogang, A New Clustering Algorithm of Preserving the Original Data's Privacy, 2008.

[6] Ali Inam, Selim. V. Kaya, Privacy preserving clustering on horizontally partitioned data, Data & Knowledge Engineering, vol.63, pp. 646-666, 2007.

[7] http://www.cse.unr.edu/~bebis/CS302/image_info.html

Authors' Profile

MaramBalajee, working as an Sr. Asst. Prof in GMR Inst. Of Tech., Rajam, Andhra Pradesh, INDIA. Obtained his degrees in M.E (CSE) from Anna University, Chennai, MBA(GENERAL) & MA(MCJ) from Alagappa University, Karaikudi. Now he is pursuing P.hD(CS) Part-Time from Bharathiar University, Coimbatore, Tamil Nadu. He Published 15 research papers in International / National Journals / Conferences.

Dr. ChallaNarasimham obtained Ph.D (Computer Science) in the year 2009, after completion of his MCA and MTech(IT) degrees. Currently, working as rofessor in S R Engg College (Autonomous) .Warangal, INDIA. He is having about 18 years of experience in industry & Teaching. He has published more than 31 papers in International / National Journals / Conferences.