International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

ENCRYPT AND DECRYPT IMAGE USING VIGENERE CIPHER

Vaka Vamshi Krishna Reddy[1], Sreedhar Bhukya[2],
[1]Student,[2]Professor,
Department of Computer Science and Engineering,
Sreenidhi Institute of Science and Technology,
JNTUH Hyderabad, India.
vamshikrishnareddyvaka@gmail.com

May 23, 2018

Abstract

This paper proposes a method to encrypt an image based on one of the primitive text encryption algorithms, the Vigenere Cipher. The digital image is first converted to Base64 format. Then, this representation of the image acts as an input file for encryption. The characters in the Base64 file are substituted based on the pre-created character table and the Cipher key. The encryption process used here is Vigenere poly-alphabetic substitution where a single character is substituted by more than one literal at different parts of the Base64 text using a symmetric key– same key is used for both encryption and decryption. The resultant so formed is cipher text which is transmitted over a medium to the receiver. At the receiver end, the same key and table is used to decrypt the received text and convert it to actual Base64 of the image. This decrypted Base64 is then converted back to readable image formatjpeg, png. So far, Vigenere cipher has been used for text encryption. By making some modifications to this algorithm, it can used for image encryption.

***Key Words*:**algorithm; Base64; character; cipher; decrypt; encryption; image; poly-alphabetic.

1 Introduction

Today, the world is all about data. Almost everything we do is being recorded some way or the other .The field of data science is booming and is showing its potential to better understand and foster the human race, devise plans to improve business, in artificial intelligence (AI) to challenge human intelligence [1]. Thus, Data has an eminent role in this digital life and it is necessary to maintain the integrity of data to achieve the desired outcome. Data in the form of text, images, videos and audio is multiplying exponentially. So, there is a need to store, maintain and secure this incessant data efficiently to ensure data integrity. Digital images are one of the commonly used data. These are produced at an increasing rate from numerous sources and are transmitting over unreliable media to reach diverse destinations .When reaching from source to destination, there is a threat of intruders accessing the image [2]. In order to prevent this third-party intervention, there is a need to encrypt the image, so that, it will not be in intelligible form even if the intruders can have it. So far, many image encryption techniques are proposed based on the properties of the pixels in the image [3]which may be difficult to understand and complex to implement.

2 EXISTING WORK

Encryption is a technique that is being used since ages to prevent unauthorized access of data. Vigenre cipher ,a poly-alphabetic cipher, uses a symmetric cipher key for encrypting and decrypting the text[4].It is very easy to understand and implement. It remained unbreakable for centuries and is more resistant to letter frequency analysis than the simple alphabetic substitution.

Vigenere cipher uses a 26 26 tableau as shown in figure 1.This technique uses a key to encode the data of a text file. The alphabets of the key are used sequentially and then repeated in cycle. So, the position of each plaintext character in the source string determines which mapping is applied to it. Thus, based on the characters of the key and the tableau contents, the original content of the text file are replaced by the cipher text and making it illegible.

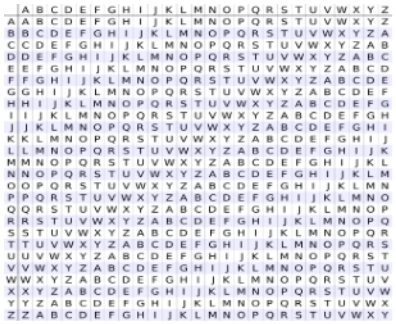

Figure 1 Tableau for text encryption in Vigenere Cipher

3 PROPOSED APPROACH

The proposed method uses the concepts of Vigenere cipher for encrypting the image following the same text encryption steps. An image chosen by a sender is the primary input. The binary representation of this image is extracted. But, working with this Base2 is not easy. So, we need to choose a system which is easy to apply the Vigenere cipher. Choosing Base8, Base16 or Base32 representation of the image is not much benefit as the number of characters that are produced on conversion for an average quality image to the corresponding format can be a few lakhs. Encrypting this bulk of characters may take time and space. Moreover, they are easier to crack as the number of combinations of characters in these systems is less. So an affordable format, Base64 is chosen [5]. Base64 is an encoding scheme designed to allow binary data to be represented as ASCII text. Even if we go for the Base64 format, we may get tens of thousands of characters. But it is quick and easy when compared to the other conversions. Vigenere cipher for text uses 26 26 character table. In the proposed Base64 algorithm, a table with 64 rows and 64 columns is used. Each row in the table is comprised of characters 'A' to 'Z', 'a' to 'z', 0 to 9,+, /.These 64 characters can be in any order in each row. Jumbling of characters, unlike the traditional Vigenere cipher, in each row makes the cipher text difficult to crack. For indexing, alphabets 'A' to 'Z', 'a' to 'z', 0 to 9, +,/ in the same order are used as indices for both row-wise and column-wise. The column indices are used as an index for plain

Base64 text and the row indices as an index for the cipher key. The 64 64 table so formed is known as tableau which acts as a reference for text substitution. The receiver must have the clone tableau as the sender to decode the encrypted file. These protocols are agreed upon by both the parties forehand the actual transmission. The Base64 image is the input for the text-replacement algorithm. The sender gives a key to encrypt in the Base64 format. The more the number of characters in the key, the more it is difficult to crack the cipher text. The first character in the Base64 text of the image is taken. It is checked with all the indices in the column to get the corresponding column number. Suppose the character is W The column number will be 23. Now, the index of the first character in the key in row-wise is found out. Suppose the character of the key is +, then the index will be 63. Now in the tableau, the element corresponding to column number 23 and row number 63 is replaced with the character in the Base64 text. In our example, 'W' will be replaced by the corresponding element in the cell. For the subsequent characters in the Base64 text, the process is repeated. In this process, if the end character of the key is reached, we start with the first character of the key again. Thus, the characters of the key are used in a cyclic manner. Thus, each and every character the plaintext is replaced by the corresponding character in the tableau. At the end of this step, we will get the encrypted Base64 version of the image. This image can be transmitted over a transmission medium. At the receiver end, the process is similar but in a reverse way. The receiver must use the same cipher key and the same tableau to get the exact image as sent by the sender. The index of the first character in the key is found out. In our example, it is 63. Now in this 63rd row of the tableau, the first character of the key is searched to get the column index. The column character corresponding to this index is the actual character in the Base64 text. For the subsequent characters, this process is applied to obtain the actual Base64 text of the image dispatched by the sender. This decrypted text is converted back to readable image extensions.

4 RESULT

Both the sender and the receiver must follow the same protocols viz. Tableau and the Cipher key

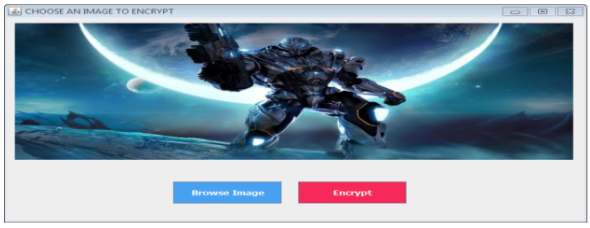

Figure 2 Image chosen by the Sender

The image which the sender wants to send is chosen by the sender

Figure 3 Image shown as Base64

The Image chosen is converted into Base64 format for Encryption step.

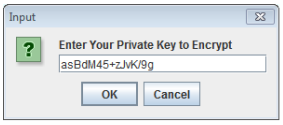

Figure 4 Sender enters the encryption key

The sender then encrypts inputs the private key to start the encryption process.

Figure 5 After encryption,the image cannot be read

Using the tableau and the Cipher Key, the encrypted Base64 format of the image–not readable– is formed and is send to the receiver.

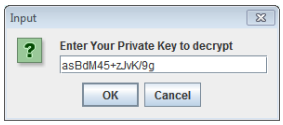

Figure 6 Decryption key entered by the receiver

At the receiver end ,the receiver inputs the same key and decrypts using the same tableau as reference

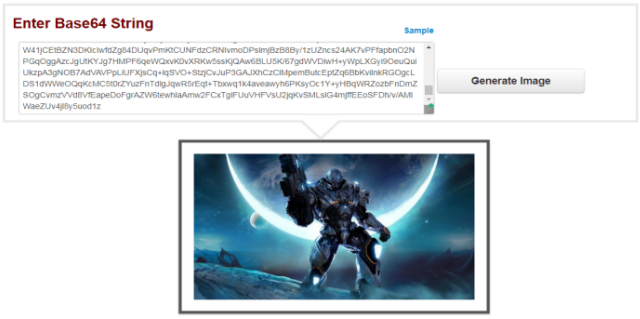

Figure 7 Receiver can read the image after decryption

The original Base64 content is extracted and the image is obtained The Base64 algorithm provides two-layered protection. The first level defense is offered by the Cipher key –as in Conventional Vigenere. The second is achieved with the tableau. For each character in the plaintext, the tableau offers 64 characters for substitution. Thus, there is a tremendous increase in the character combinations as compared to the usual Vigenere–making Base64 difficult

to crack. Also, traditional Vigenere has 26 26 tableau with an ordered arrangement of alphabets. In the proposed algorithm, the 64 characters of each row are jumbled. Thus, each sender-receiver pair has distinct tableau, further enhances the security. In conventional Vigenere Cipher, the characters in the plaintext have a meaning. It is simply the structured English language. Lack of randomness in plaintext makes the encrypted text a prey for frequency analysis. Frequency analysis compares the frequency of alphabets in the encrypted text with the frequently used English alphabets. Suppose, an encrypted text of an English message has the most frequent alphabet as K, the K is replaced by E.E, being most frequently used alphabet in the English Language, may come in place of K. It can be said that traditional Vigenere is not immune from Frequency analysis. On the other hand, the proposed algorithm works on image data and so frequency analysis may not work. Each image has different sizes, divergent pixel colors, intensity values [6].If the image is plain, the pixels, and thus, the corresponding Base64 will be repeated. So, the image may be cracked. But in reality, the images are complex with non-uniform color distribution .Hence, it may not be possible to guess the image. Caesar Substitution Cryptograms (CSC)[7] may not be able to crack the proposed algorithm for the complicated color-distribution image.

5 FUTURE SCOPE

Vigenere cipher remained un crack able for centuries. But was later cracked by frequency analysis and also by guessing the key length and then applying the CSC. So, if we make Vigenere cipher in such a way that it cannot be used cracked using frequency analysis or CSC, in future, we may use it for securing other complex types of data viz audio, video by applying alterations to the algorithm. Nothing is impossible in this digi-world. One day this algorithm may be cracked. Hope that day will be far.

6 ACKNOWLEDGEMENT

My sincere thanks to Dr.B. Sreedhar ,Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science

and Technology for his inspiration and support.

References

[1] Saporta. Training Data Scientists:A Few Challenges. G. Int J Data Sci Anal, 2018.

[2] Vineeth V,N.Radhika, V.Vanithaa. Intruder Detection and Prevention in a Smart Grid Communication System. Procedia Technology, 2015.

[3] Jian Zhang and Yutong Zhang. An Image Encryption Algorithm Based on Balanced Pixel and Chaotic Map. Mathematical Problems in Engineering, 2014.

[4] Aized Amin Soofi, Irfan Riaz, Umair Rasheed. An Enhanced Vigenere Cipher For Data Security. International journal of scientific technology research, 2016.

[5] Isnar Sumartono , Andysah Putera Utama Siahaan , Arpan. Base64 Character Encoding and Decoding Modeling. International Journal of Recent Trends in Engineering Research (IJRTER), December 2016

[6] Pike, Steven D. Destination Image Analysis: A Review of 142 Papers from 1973-2000.

[7] https://simonsingh.net/cryptography/cryptograms/, Figure 1: https://en.wikipedia.org/wiki/Vigen