LETTER FREQUENCY DEPENDENT CRYPTOGRAPHY TECHNIQUE

Akshat Kapoor[1], D Shruti[2]

[1,2]CS, B.tech, IPEC, UP, (India)

ABSTRACT

The advancement of technology, the Internet, and information sharing has had both positive and negative impacts. One of the negative impacts was the massive increment in fresh information threats. The number of threats and reported computer related incidents increased by an overwhelming rate by the end of the 1990's, and the 2000's. Many of the computer incidents misused confidential information that was stored by companies in a variety of different industries. Sharp increase in system vulnerabilities has made the ability to carry out threats against information system easier. Weak or non-existent information security practices were also resulted by unauthorized access to confidential information. In order to make information system more secure different techniques were introduced. Now day's every little data that is shared or stored is encrypted in one or the other way to make it more efficient and secure. New encrypting techniques are introduced to make information system more protected.

Keywords: Baudot Code, Cryptography, Huffman Algorithm

I. INTRODUCTION

Cryptography is an art of securing information from unauthorized access. It is also a storing and transmitting data method in a particular form in which only those for whom it is destined for can read and process it. The first registered use of cryptography is dated back to 1900 B.C. when non-standard hieroglyphs were used by Egyptian in an inscription. As the computer communication systems started fast emerging new forms of cryptography are being introduced. In data and telecommunications, cryptography is crucial when communicating over any unauthorized medium. Classic securing communication methods are mainly base on cryptography .In which encrypts plain text encrypted to cipher text. However, the transmission of cipher text may easily fire up the attackers and thus the cipher text may be attacked, intercepted or decrypted violently. In order to make up for the shortcomings of cryptographic techniques, various algorithms are introduced and developed in order to improve security.[1][2] Cryptography had a major turn when Huffman was introduced. Huffman algorithm was presented by David A. Huffman in a 1952 paper. His method attracted an large amount of research and it is used in many applications such as data compression techniques and fax machines, especially image compression, is the main contribution of this work. The two properties of Huffman coding they are used usefully important are unique prefix property, where not Huffman code is prefix of any other Huffman code, and idealism, where the Huffman code is minimum-redundancy code. [3] In digital telegraphy a standard 5-bit code is commonly used to represent a character this code is primarily known as the Baudot code but this name is not from the beginning the official name for the latest telegraphy standard is International Telegraph Alphabet No 2(ITA2). Then ASCII in 1963, but is still used by amateurs today. The most common Baudot code

is also referred as Murray code, or as Baudot-Murray code. The ITA2 standard is used widely with historical cipher machines. [4]

II. TEXT TO IMAGE USING BAUDOT CODE

In this research paper we are going to work in technique to covert a text file or bunch of characters to image in other words encrypting the character in such a way that image is formed, that could not be understood by normal users who access that file. As the Baudot code are well known in field of communication, as it encrypts in the form of circles. So, Baudot codes can be modified and used to make image from text.

Steps for forming image from text can be as follows:-

Step 1: Basic Algorithm of Baudot Murray code can be used to convert text into encrypted result. Result image formed would be like figure 1 given below.

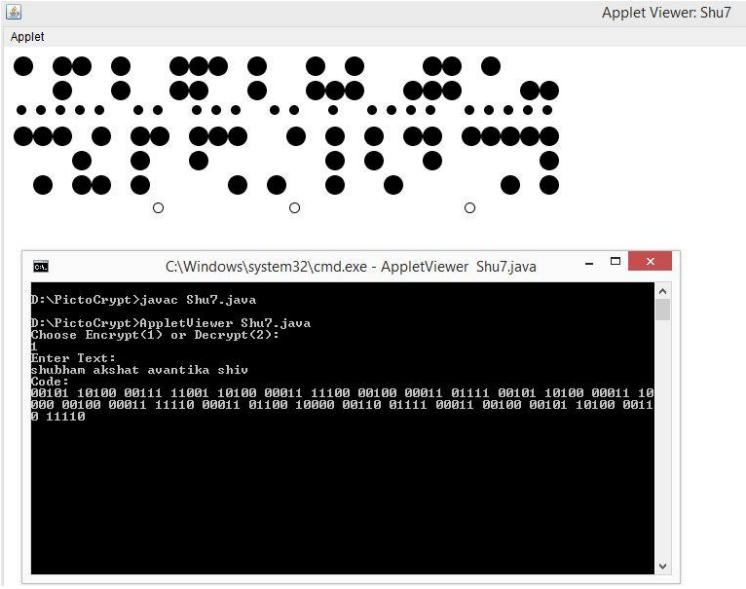

Figure 1- Text to Baudot Code

Step 2: Only basic changes in algorithm can be done in order to convert the above Baudot code in a colorful image. So, the resulted image will be as figure given below.

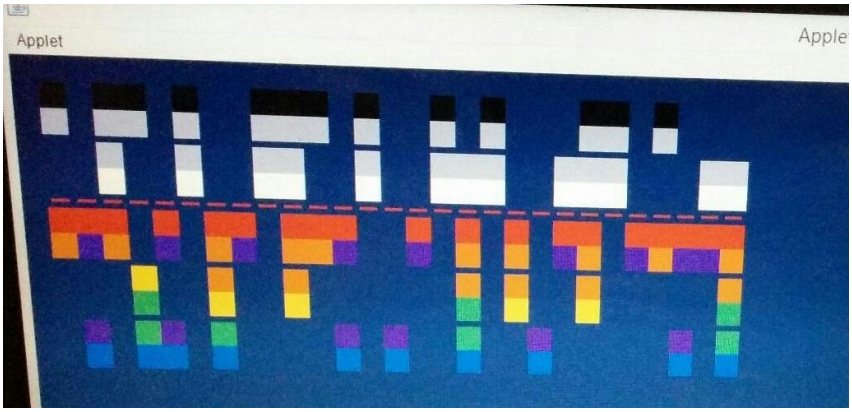

Figure 2- Text to Image

 ISBN: 978-81-931039-7-5

III. LOOP HOLE OF THE TECHNIQUE

Steps used above to make an image formed have some drawbacks. If we input a character "s" then image formed by above technique will always be like figure 3.

Figure 3- Image of letter "s"

So, risk of decrypting of result by unauthorized user will increase. To reduce this hacking risk security must be improved.

IV. IMPROVING SECURITY BY HUFFMAN TECHNIQUE

To improve security we can adapt frequency depending encoding by using Huffman algorithm. Huffman algorithm is given below.

```
Huffman(C)
n=|C|;
Q=C;
for i: = 1 to n − 1
do
allocate a new node z
z.left = x = Extract-Min (Q);
z.right = y = Extract-Min (Q);
z.freq = x.freq + y.freq;
Insert (Q,z);
end for
return Extract-Min (Q);
```

Here Q is the priority queue which is filled according to the frequency of character. As we can note that character are stored in binary tree. Huffman is used for compression so; prefix codes are used as they simplify decoding. Binary code words for path from root to character can be given as 0 for left child and 1 for right child as shown in figure4. For instance a string 001011101 can be decoded as aabe. This is dependent on character frequency so its code may change depending on text given as input.

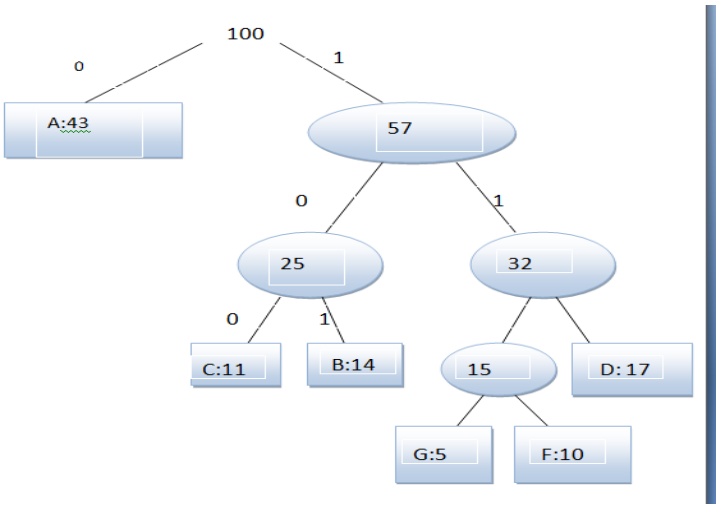

Figure 3- Prefix Code Applied by Huffman algorithm

Now, if we assign Baudot image for each binary code security will increase. That is if we input some sting of characters then it is possible that every time a particular character may show different image. This is how a basic file compressing technique can be used for improving data securing cryptography technique.

V. CONCLUSION AND SUGGESTIONS

Technique defined in this research paper can increase security of the text file that is transferred from one user t another. Steganography can also be used to give double layer encryption. Steganography is a science of communication in such a way that hides the existence of communication. In other words it is a process in which a massage is hidden within a image. [5] So, what can be done the image formed by the above technique can be encrypted by using Steganography which will give double level of encryption. This will increase data security to a large height.

REFERENCES

[1] NOVEL SECURITY SCHEME FOR IMAGE STEGANOGRAPHY USING CRYPTOGRAPHY TECHNIQUE, Lokesh Kumar Volume 2, Issue 4, April 2012 ISSN: 2277 128X.

[2] A SURVEY ON VARIOUS CRYPTOGRAPHY TECHNIQUES, Mitali, Vijay Kumar and Arvind Sharma, Volume 3, Issue 4, July-August 2014.

[3] FINGERPRINT PATTERNS RECOGNITION SYSTEM USING HUFFMAN CODING, Abdurazzag Ali Aburas and Salem Ali Rehiel, World Congress on Engineering 2008 Vol III WCE 2008, July 2 - 4, 2008, London, U.K.

[4] http://www.cryptomuseum.com/crypto/baudot.html

[5] IMAGE BASED STEGANOGRAPHY AND CRYPTOGRAPHY, Domenico Bloisi and Luca Iocchi, Sapienza University of Rome, Italy.