International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

3D-CRYPTOGRAPHY

Karan Bhatt[1], Mahesh Haravade[2], Samanata Pednekar[3], Mansi Shinde[4] & Prof. Dr Varsha Shah[5]

[1-4]Dept. of Electronics & Telecommunication Engineering
[5]Principal, Rizvi College of Engineering
Rizvi College of Engineering, Rizvi Complex, Bandra West Mumbai, India.

Abstract - *Digital communication has become an essential part of the infrastructure in the present world and it has witnessed a noticeable and continuous development in a lot of applications during the last few decades. Cryptography distorts the original message itself whereas steganography hides the existence of the message. In the present scenario, any communication of internet and networks application requires security as it is a very much crucial part of a network. In our research, we aim to develop an algorithm or a technique which includes the benefits of both cryptography and steganography in order to provide a better result. It incorporates one of the most secure algorithms known as Advanced Encryption standard (AES) which is our main encrypting tool. The resulting encrypted message is converted into a three dimensional array which is then embedded into the image for additional security by using the concept known as bit plane slicing. The thing that makes our proposed model different than the various conventional cryptographic techniques is that it gives two layers of security for secret data or the data which is to be transferred, which fully satisfies the basic key factors of information security system which includes: Confidentiality, Authenticity, Integrity and Non – Repudiation.*

Key Words: **Cryptography, Steganography, Advanced Encryption Standard, Bit plane slicing, 3D array, Confidentiality, Authenticity, Integrity**

1. INTRODUCTION

In today's age, the concept of data transmission from one side to the other by conventional means has been changed thanks to the Internet and communication technologies, resulting in improved protection of information being transmitted over the Internet, as sensitive data must always be transmitted safely over the Internet while preserving confidentiality, integrity and availability. Digital communication has now become an integral part of the network. A large number of applications relying on the Internet and communication is vital to be kept secret. Cryptography and steganography are commonly available methods for data protection. Cryptography requires translating a text of a document into an illegible cypher. On the other side, steganography is a digital media that covers technology. Compared to cryptography, a message or authenticated code is inserted into a digital host before it is sent over the network and therefore there is no established life. It deals with developing and analyzing protocols which prevent malicious third parties from retrieving information being shared between two entities thereby following the assorted aspects of knowledge security. Secure Communication is the sharing of data or message between two parties which cannot be acquired by any other source. Cryptosystem uses one algorithm for encryption and another for data hiding and also involves private key generation for data encryption/decryption. These all processes are embedded in one protocol and programmed in software which works on operating systems. This paper focuses on the effectiveness of integrating cryptography and steganography methods to improve the security of information over an open channel.

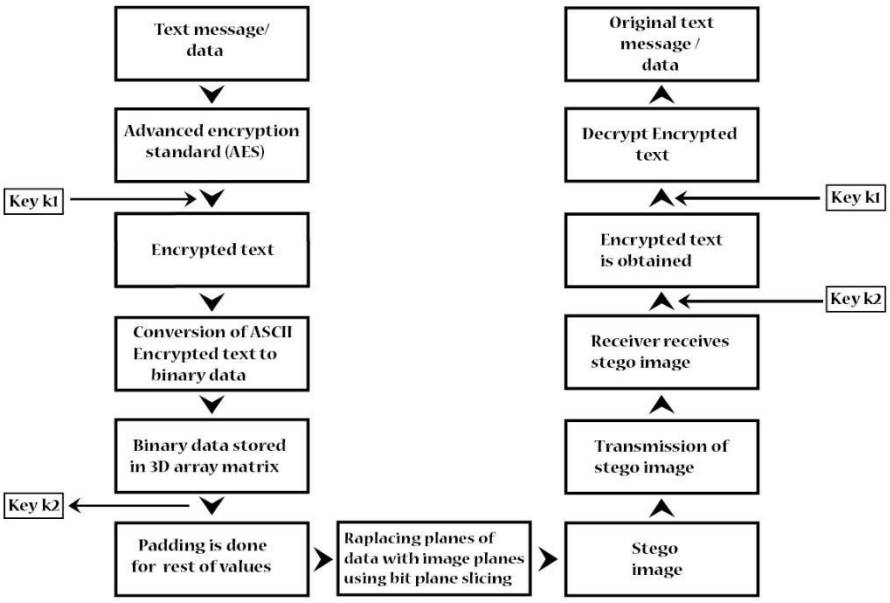
1.1 Materials Required

At one hand, there are different programming languages one can choose for developing security algorithms and on the other hand, there are various cryptographic techniques available for the same. Choosing the right one will make the implementation of algorithms simple and secure. In our project, we didn't use any hardware components.

A. Software Requirements

● JavaScript: JavaScript is an easy-to-use programming language. It can enhance the dynamics and interactive features of your page by enabling you to perform calculations, check forms, add special effects, create security passwords, and more.
● Crypto.JS: Crypto.JS is an expanding collection (library) of standard and safe cryptographic algorithms enforced using best practices and patterns in JavaScript. They are fast, and their interface is compatible and convenient.
● Plotly.js: Plotly.js is an excellent library for JavaScript applications that make use of graphs and charts. Plotly.js allows web graphs of interactive, publishing quality.

1.2 Methodology



To better understand the working of the algorithm, we split it into two parts as follows ;

A. Encryption process :

- The data or the message which is to be sent secretly is first encrypted with the help of a known algorithm called Advanced Encryption Standard (AES).
- The reason for choosing AES for our current project is that AES is a fast, secure form of encryption and it is a widely used algorithm that keeps eyes out of our data. Various versions of the AES algorithm are available at present such as 128, 192 and 256 bit depending on the key size. We have used the 192-bit version. Encryption is done with key k1.
- As a result of the AES, we get the encrypted text. Next, we are dealing with the array part for which the text or the ASCII form of encrypted text needs to be converted into binary form in order to store data in a 3D array.
- Once the data is placed in a 3D array the positioning, the data gives us the key 2 which will be shared with the intended recipient and used during the decryption process. Data padding is done for the rest of the values in the array.
- Next, comes one of the most important parts of the project which is steganography. The planes of the 3D array are embedded on the image planes with the help of a technique called bit plane slicing.
- Bit plane slicing is a way to represent an image with one or more bits of the byte used for each pixel. MSB of the byte carries visually most significant data and this significance reduces as we move from the MSB to LSB. So we can replace the last two to three planes of the image without knowing either one.
- This gives us a stego image where our secret message is hidden which can be sent to the intended recipient.

B. Decryption process :

- Once the intended recipient gets the stego image, he/she uses the key k2 which is generated during the encryption process to obtain the encrypted text hidden into the image.
- The important point to notice here is that the key k2 used on the 3D array is only related to the desired encrypted data present into the array and only retrieves desired AES encrypted data thus reducing the overall decryption time. The obtained data is then converted to the ASCII form.
- As AES is a symmetric key algorithm, the key k1 which is used during the encryption of the text is also used for the decryption of the text.
- The recipient decrypts the text and he/she gets the message from the sender.

- The steganography makes the message or data imperceptible to the attacker and even if the attacker detects the transmission of data or message the cryptography will secure the data with encryption.

1.3 Implementation

To understand how to encrypt data in a three-dimensional space, one can visualize the data being segregated into its very raw form, that is, 1's and 0's. This data is placed into a cube with cells. Each cell can only contain either a one or a zero. So the first part of the process remains conversion into binary format. Once that has been achieved, we can start inserting the numbers into an empty three-dimensional matrix in a randomized format. The size of the cube (total number of cells) has to be larger than the input data. Ideally, the bigger the size of the cube, the better is the strength of the encryption. That consumes a lot of processing power and hence, this formula is used for deciding the size of the cube for general computing systems.
Cube side size = ceiling (cube root (binary message length))+5
The encrypted data is then applied on the back of an image whose size should be larger than that of the cube. The sender sends the key and image to the recipient. The key contains both the aes password and the key for the 3D algorithm.
Decryption process on the recipient side relies on the image and the key. The encrypted data is extracted from the image and decryption algorithm is applied to it to receive the original text back.

2. OBSERVATION

For Encryption:

	MESSAGE SIZE (IN CHARACTERS)				
CUBE SIZE	100	200	300	400	500
13	5.2 ms	6.1 ms	7.9 ms	10.1 ms	9.5 ms
14	7.4 ms	7.2 ms	10.7 ms	14.1 ms	15 ms
15	8.9 ms	8.6 ms	13.2 ms	18.2 ms	19.9 ms
20	19 ms	18.3 ms	29.7 ms	37.8 ms	47.8 ms
30	47 ms	57.4 ms	83.8 ms	108.1 ms	132.3 ms
40	95.2 ms	129.1 ms	188.9 ms	256.3 ms	310.6 ms
50	169.7 ms	248.5 ms	367.4 ms	482.5 ms	724 ms
60	280.2 ms	514.5 ms	646.9 ms	833.9 ms	1219.6 ms
70	452.1 ms	818.7 ms	1004.2 ms	1326.9 ms	2060.2 ms
80	632.7 ms	1137.7 ms	1499.3 ms	2212.3 ms	2919.5 ms
90	801.3 ms	1482.3 ms	2193.6 ms	3107.5 ms	3621.5 ms
100	1047 ms	1974 ms	2919.5 ms	4532.7 ms	4854.2 ms

Table 1 : Time for Encryption for password size of 30 characters

For Decryption:

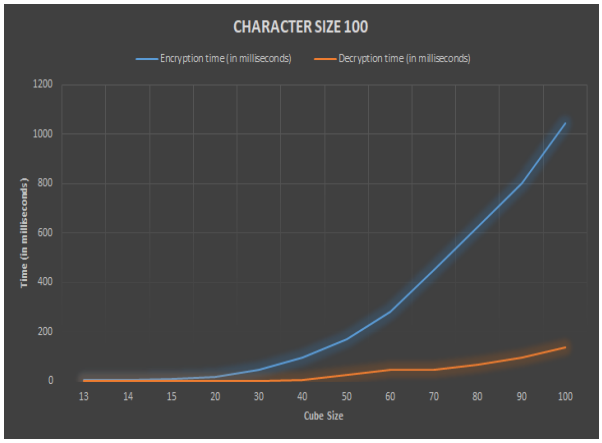
	MESSAGE SIZE (IN CHARACTERS)				
CUBE SIZE	100	200	300	400	500
13	0.8 ms	0.7 ms	0.7 ms	1.3 ms	0.6 ms
14	0.4 ms	0.6 ms	1 ms	0.9 ms	2 ms
15	0.7 ms	1 ms	0.8 ms	0.8 ms	2 ms
20	0.9 ms	1.6 ms	1.4 ms	0.7 ms	2.1 ms
30	2.6 ms	1.9 ms	2.3 ms	2.1 ms	2 ms
40	4.9 ms	5 ms	4.8 ms	12.6 ms	6.3 ms
50	28.1 ms	26.3 ms	23.3 ms	38.8 ms	35.8 ms
60	48.1 ms	56.2 ms	36.3 ms	35.6 ms	84.3 ms
70	48.1 ms	52.3 ms	55.4 ms	67.4 ms	80.8 ms
80	65.8 ms	67.2 ms	72.4 ms	90.6 ms	78 ms
90	97.8 ms	102.7 ms	111 ms	97.4 ms	136.3 ms
100	135.8 ms	139 ms	135.3 ms	100.5 ms	142.7 ms

Table 2 : Time for Decryption for password size of 30 characters

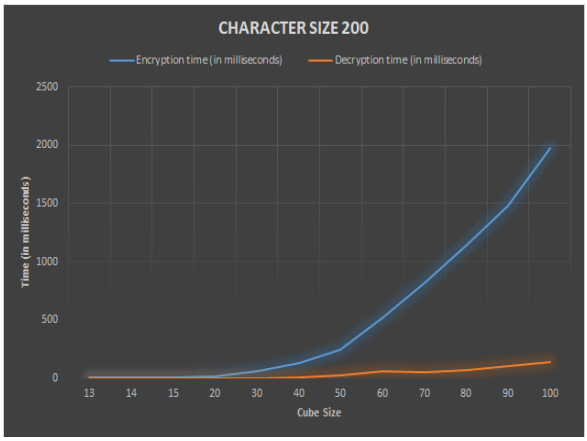
(Note: All the observations are recorded in a Lenovo device called Ideapad 330-15IKB. These observations can vary from device to device depending on the specifications, processing speed and capacity of the device)

3. RESULTS

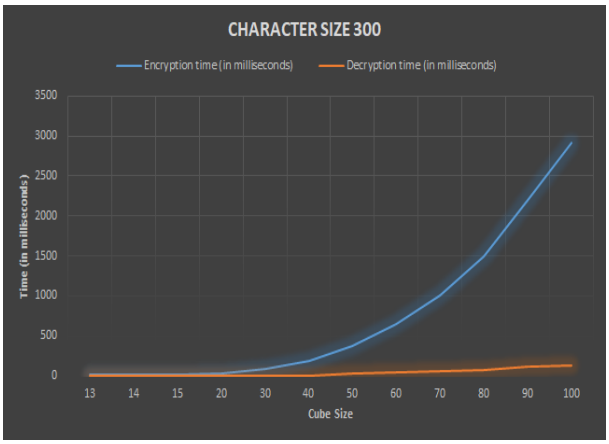
The speed of the encryption and decryption for the above algorithm varies from device to device. It depends upon the various specifications of the device such as the computational speed, capacity, processor and many more. During the encryption process, the formation of 3D cube takes place with the help of intended encrypted messages bits and padded bits whereas during decryption only the intended message from the cube is retrieved. This in turn, reduces the time required for the decryption which can be seen from the above observation table. Thus the overall time period required for the algorithm is reduced making the algorithm faster.



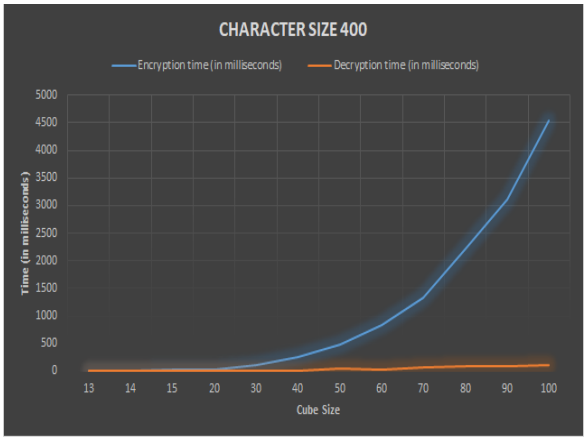
1: Encryption and Decryption time for character size 100



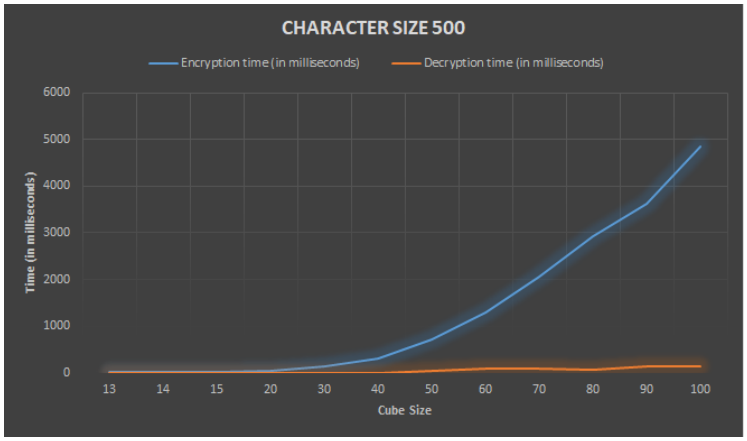
2: Encryption and Decryption time for character size 200



3: Encryption and Decryption time for character size 300



4: Encryption and Decryption time for character size 400



5: Encryption and Decryption time for character size 500

4. CONCLUSIONS

Most of the security algorithms available today are fast but they are not secure enough, resulting in a data breach; only some of them are secure. In such cases, '3D cryptography' plays an important role by providing a better option, resulting in a combination of both security and faster speed. '3D Cryptography' which helps in employing steganography with ease, providing two layers of security making it more secure. The retrieval of messages is much faster as well. Therefore '3D cryptography' has a wide variety of applications which includes military use, digital signature, authentication, time stamping, etc.

REFERENCES

[1]. Rashad J. Rasras, Ziad A. AlQadi, Mutaz Rasmi Abu Sara, "A methodology based Steganography and Cryptography to protect highly secure messages" Engineering, Technology and applied science research Vol 9, No. 1, 2019, 3681-3684

[2]. R. M. Patel, D. J. Shah, "Conceal gram: Digital image in image using LSB insertion method", International Journal of Electronics and Communication Engineering & Technology, Vol. 4, No. 1, pp. 230-2035, 2013

[3]. M. Jose, "Hiding Image in Image Using LSB Insertion Method with ImprovedSecurity and Quality", International Journal of Science and Research, Vol. 3, No. 9, pp. 2281-2284, 2014

[4]. Bhinal Chauhan, Shubhangi Borikar, Shamali Aote, Prof. Veena Katankar "A Survey on Image Cryptography Using Lightweight Encryption Algorithm" IJSRSET Volume 4 ISSN 2395-1990

[5]. Secret Data Transmission Using Combination of Cryptography &Steganography Ajin P Thomas, Sruthi P., Jerry Rachel Jacob, Vandana V Nair, Reeba R IJCERT Volume 4, Issue 5, pp. 171-175

[6]. A.Nag, J. P. Singh, S. Khan and S. Ghosh," A Weighted Location-Based LSB Image Steganography Technique", Springer ACC 2011, Part II, CCIS 191, pp. 620-627, 20 II

[7]. G. Swain and S. K. Lenka, " A Technique for Secure Communication using Message Dependent Steganography", Special issue of IJCCT, Vol. 2, No. 12,2010

[8]. Odii. J. N., Hampo J.A.C, Okpalla C.L and Onukwugha C.G "Hybridization of Cryptography and Steganography for Information Security" Futo Journal Series (FUTOJNLS) Volume-5, Issue-2, pp- 227 – 234

[9]. N. Akhtar, P. Johri, S. Khan, "Enhancing the security and quality of LSB based image steganography", 5th International Conference on Computational Intelligence and Communication Networks, Mathura, India, September 27-29, 2013