ENCRYPTION THREE-DIMENSION IMAGE USING TINY ALGORITHM

M.SC Noor Hayder Abdul Ameer[1]
[1]*Department of Computer Science*
University of Technology
Baghdad, Iraq
110048@uotechnology.edu.iq

M.SC Zahraa Faiz Hussain [2]
[2]*Department of Computer Science*
Al Salam University College
Baghdad, Iraq
Msc_zahraa@yahoo.com

M.Sc May Sabri Mohammed [3]
[3]*Department of Computer Science*
University of Technology
Baghdad, Iraq
110051@uotechnology.edu.iq

Abstract **- The development of systems allows providing the capability of using three-dimension (3D) pictures over the internet especially in social media. In previous years, animation pictures and videos are not used in the internet due to the sizes of these two data and need the huge amount of data to work over internet and need supporting program to deal with presenting the data to the users of the internet in either websites or social media. Most of the security over internet used on ciphering text or ciphering images but not cipher video or 3D picture because video and 3D pictures are not used until recently. The huge use of these two types 3D pictures and videos in recent years. It is become an urgent necessary to encrypt these sorts of data. The research will focus on encrypting these types of data by using special algorithm called as Tiny Encryption Algorithm (TEA). This algorithm will be used to encrypt and decrypt 3D pictures and protecting the privacy of this sort of data. The research shows the how-to encode and decode of 3D picture and how to deal with them. The results show the TEA is rapid algorithm in the coding picture and decoding 3D pictures. it is only needing a few portions of time to cipher and decipher 3D pictures. The program that used to test the ciphering and deciphering algorithm was based on MATLAB.**

Index Terms - Tiny Encryption Algorithm, Tea Encryption, three-dimension (3D) pictures

I. INTRODUCTION

TEA is created by Wikram Reedy Andem in 2003 and the propose of this algorithm to be used in as encryption algorithm in the embedded system design. At first, the TEA is used only for ciphering only plain text [1], later the TEA is used ciphering for images [2]. The uniqueness of TEA, it is rapid chippering of data and high performance when it works in the embedded system design and the implementation of it is very easy. Also, another advantage of the TEA is it required low power consumption and it can design in low cost [3]. Also, the TEA has the low memory usage and rapid speed of ciphering so it doesn't need large resources like others algorithm to cipher. Due to these reasons the TEA is used for ciphering 3D images. Since the type of the TEA is Feistel algorithm. This make TEA as block ciphering method. The TEA has very well immunity against cryptanalysis. The TEA used 32 rounds for ciphering any data. However [4], it can be release after the sixth round since when changing 1-bit in the plaintext to be cipher, the change is affected on the 32-bit code of the ciphering of the plain text in the output [5].

The most of the operation of the TEA that used in it is structure are XOR and accumulative and shifter which make it very well suited in work in the workstations and in the computers. Since these computers and workstations most of their processer designed to perform these types of instruction and this led to magnificent time performance in ciphering when using these types of computers. The TEA used specified Key which has length of 128 bits [6] [7]. The key is used to secure the data and give the guarantee that the structure of the TEA is safe. The basic structure of the TEA can be shown in figure 1.

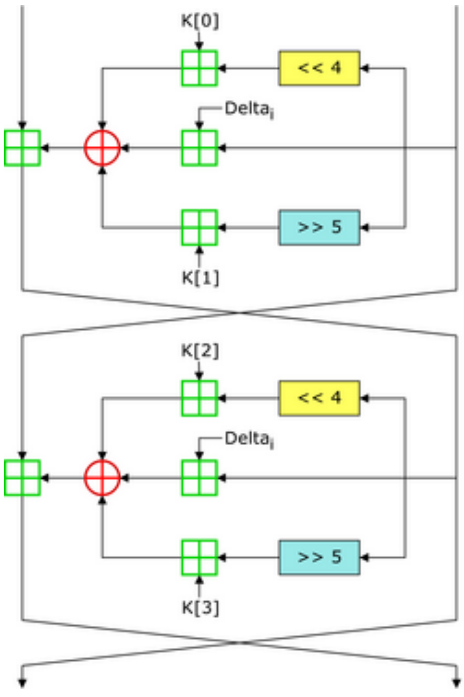

Fig 1. The block diagram of the TEA structure

In this research the system that created for ciphering three dimensions pictures is based on the TEA algorithm and the types of the images that used in the testing of the algorithm taken from random websites of social media [8] [9]. These pictures are taken based on testing the algorithm

in the field of social media and to ensure that every types of pictures can cipher and deciphering. All types of image format can be used in program. Also both color or grayscale image can be used in the program [10] [4]. The program is capably of distinguish the types of the images and find the best way for ciphering and deciphering.

II. TEA ENCRYPTION

The TEA consisted from five blocks and these blocks are combined together to produce the output of single round TEA [11]. The block are the Shifter and Delta and Key and finally the accumulative and XOR operation. At first the input that needed to be ciphered whiter plaintext or pixels it's the same it will divide every 64 bits into two parts and each part will contain 32-bits as input. The first part will be called InputRight while the second part will be called InputLeft. S, there will be two input to the TEA and these two inputs will generates Two outputs.

Since images is used in this research and image contain pixels and each pixel consist from 24 bits. The program will divide these pixels in to three 2-dimensional (2-D) matrixes. Each 2-D matrix will contain only 8 bits which represents the value of either RED, Green or Blue. These 2-D matrixes will process each one alone. The process of each of them will be the same. So that the process for producing input with 64-bits is to take 8 pixels in every ciphering steps. The eight pixels will be share between InputRight and InputLeft and each one of the well takes four pixels of one of the 2-D matrix of color values. So that InputRight will take the first four pixels and the data of the InputRight will contains pixel1, pixel2, pixel3 and pixel4. In contrast InputB will take the remaining four pixels so that the Input data of InputLeft will contains pixel5, pixel6, pixel7 and pixel8.

After producing the input data that will be ready to be ciphered using TEA algorithm in each round the InputLeft will shifted to the right by four bits and summed with the first key and then XORed with the summation results of InputLeft Data with Delta and then the results of pervious XORed will also be XORed with the summation results of shifting InputRight data to the left by 5 bits and added with the second Key. Then the results of these three operations will be summed with InputLeft data and stored in the InputLeft data as output as shown in the equation1 while the InputRight data will have the same operation but it will be summed with key3 and key 4 instead of key 1 and key 2. The operation done by first shifting the InputRight data to the right by 4 four bits and then summed with the third key and then it will XORed results of the summation of the delta with InputRight and the results of pervious XORed will be XORed again with the summation results of shifting the InputRight data to the left by five bits and added to the fourth key. The final operation will be summed the InputRight data with the XORed data that came from the previous three operations as shown in equation The results will be stored in the InputRight data. Then the delta accumulated in every round by its self.

InputLeft += ((InputLeft<<4) + Key1) | (InputLeft+delta) | ((InputLeft>>5) + Key2)------1

InputRight +=((InputRight<<4) + Key3) | (InputRight+delta) | ((InputRight>>5) + Key4)---2

The same operation will be repeated for 32 times and the output ciphering will be divided in two parts as shown in the previous equations. The first ciphering will be inside the InputLeft. Since the InputLeft data is always stored the summation in side it be the ciphered output for the he results of this will be of the after summation the to the ciphering all these pixels, the next will ciphering the next 8 pixels in the first row and so on. The ciphering will continue until finish ciphering all the pixels row after row.

The color image will be ciphered in the same process. since each pixel in the color image consist from three color which are Red, Green, and Blue so the operation will cipher each color alone. At first it will extract the three color from image by making three images with the same size as original image. These new images will contain only the value of color that specified. Which means that the image that contain the values of the pixels of Red will be ciphered alone and then the images of the Green and the Blue will be ciphered respectively. Figure 2 shows the extraction of the color and make new images for the color images. After ciphering all images color, it will return in the same process to be return as colored image again.

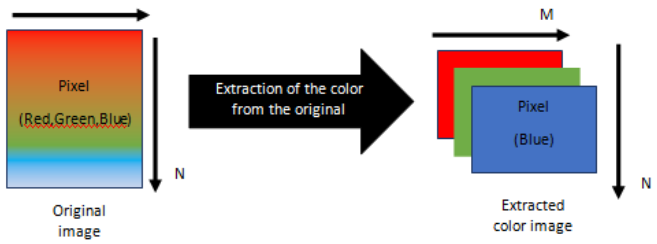

Fig. 2. the extraction process of the colour image.

The deciphering of the TEA is the same of the as encryption but in reverse way. The only change is that the value delta will be shifted to the left by 5 bits before the operation of the rounds is started and each round the value of the InputRight or InputLeft will be decrement from the total results

of XORed operation. The equation of deciphering is shown in the below in equation3 and equation4.

InputLeft -= ((InputLeft<<4) + Key1) | (InputLeft+delta) | ((InputLeft>>5) + Key2)------3

InputRight -=((InputRight<<4) + Key3) | (InputRight+delta) | ((InputRight>>5) + Key4)---4

At last, the process of the ciphering 3D images is similar in ciphering of the images the only difference is that the 3D images contain multiples images in single images and that images allow to motion the image. For example, if the 3D image is color image it will contains 4-dimensional matrix instead of 3-dimensional matrix the last column is determine the number of pictures inside the 3D images and as same way the gray image is consisted from 3-dimensional matrix not 2-dimensional image the last column will represents the number of pictures inside the 3D images. The program in this research will first determine how many images is consist and based on this will cipher each image by call up each image alone. So, the number of images will be ciphered one after one as the sequence of the images is sorted in the image. The holy process is shown in figure 3. As shown in figure 3 only one image will be selected at a time to be ciphered and when this image is ciphered the next image will be selected to be ciphered until all images that consisted of 3D images ciphered. The same operation will process on the deciphering process just make deciphering for the same way of the ciphering but in reverse order.

Results

The TEA is very rapid algorithm for ciphering and deciphering of plaintext and images. However, this program increased the speed of the algorithm since it used 8 pixels as its plain text this led to speed the performance of the algorithm by eight times faster. Since, each eight pixels is used in every ciphering process. the algorithm provides low memory usage when dealing in large pictures due to its flexibility and its structure. The results of the program on gray images is shown in figure 4. As it can shown from the figure that original image will have two ciphered images. These images represent the outputRight and outputLeft which represent the final Round from InputRight and InputLeft respectively.

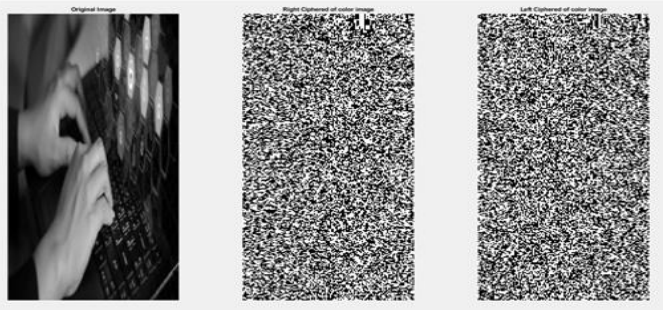

Fig. 4. the ciphering of gray image pictures

While the second results(in figure 4) of the image pictures it can shows in figure 5. It can be shown that there are 8 ciphered images ever two represent the left and the right ciphered of RED and Green and Blue images respectively. While the last two ciphered images represent the left and right ciphered images for the original image.

The results show each picture will ciphered in two part and the size of each part will be half of the pixels of the original image. This due to the fact that the combination of both ciphered image the left and right will result the same pixels of the original image. To ciphered the image of 3D, it required 29 images to be ciphered for the images below in figure 6. The ciphering done by ciphered picture after picture. The output of the ciphered image will be 58 each picture of 29 will have 2 pictures. So, the output results of images will be 58 images, 29 for the left ciphered image and 29 for the right ciphered image. The time required for each image to be ciphered is approximately 1.952 second. So, the total average for time required of all image is multiple all images by the average and the results will be 56.608 second. This time is the required time for ciphering image with size of 4096X4096 pixels. The figure 6 show only the first three images of ciphered from the total of 29 images. Table1 shows the time required for different types of images with different sizes. The results show that with the increase the size of the pixels the time required is more than the time for fewer pixels also shown in the figure the time required for the gray and color images. The testing time is based on the tic toc function of MATLAB program. The time may change according to the PC that using this program the test was done on Laptop with core i7 8850 U process and the Ram was 16 GB DDR4 and the Hard type was SSD and the Graphic card was Nvidia MX 150 with 4 Giga-Byte of RAM.

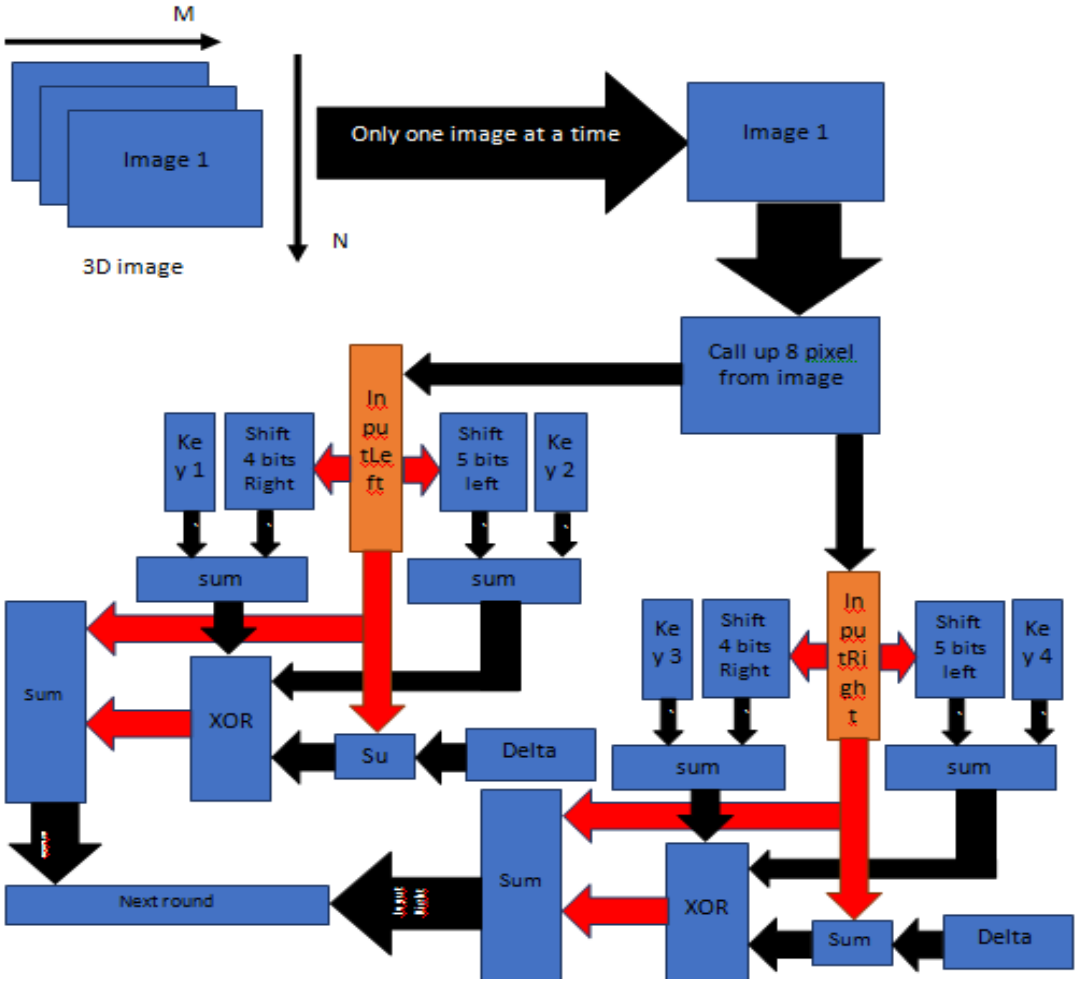

Fig. 3 the operation process for one round on 3D images

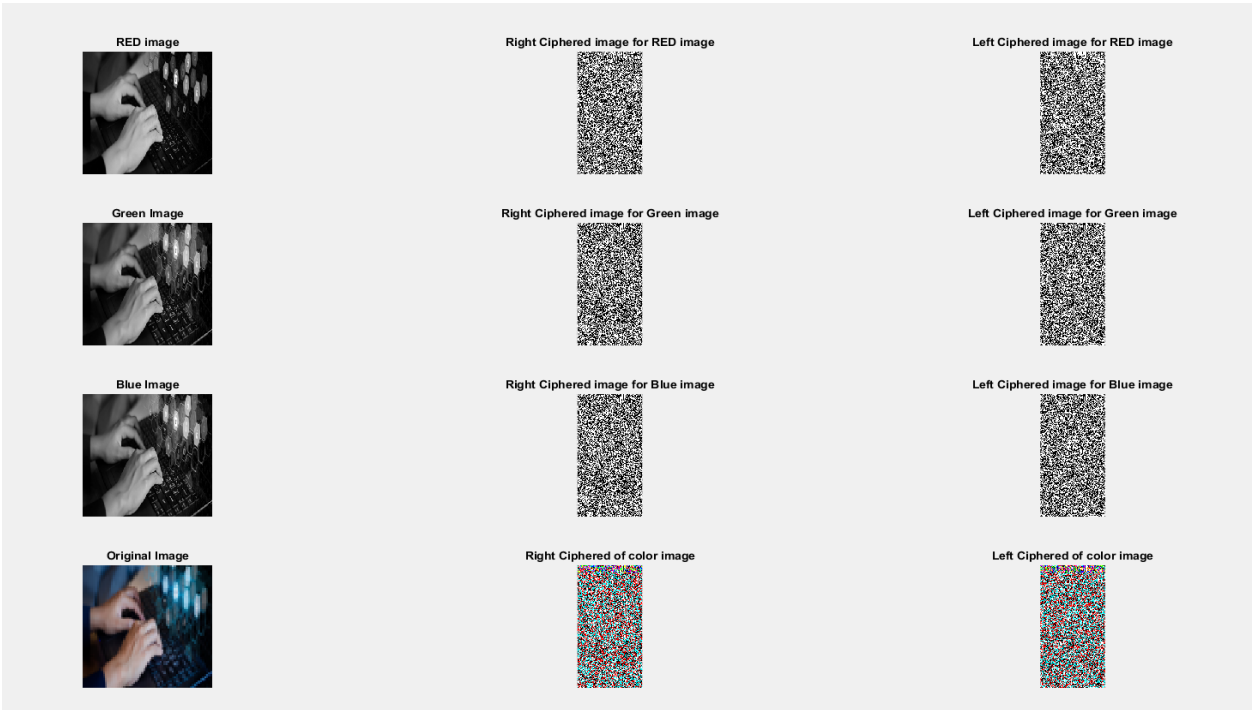

Fig. 5 The color image ciphering process.

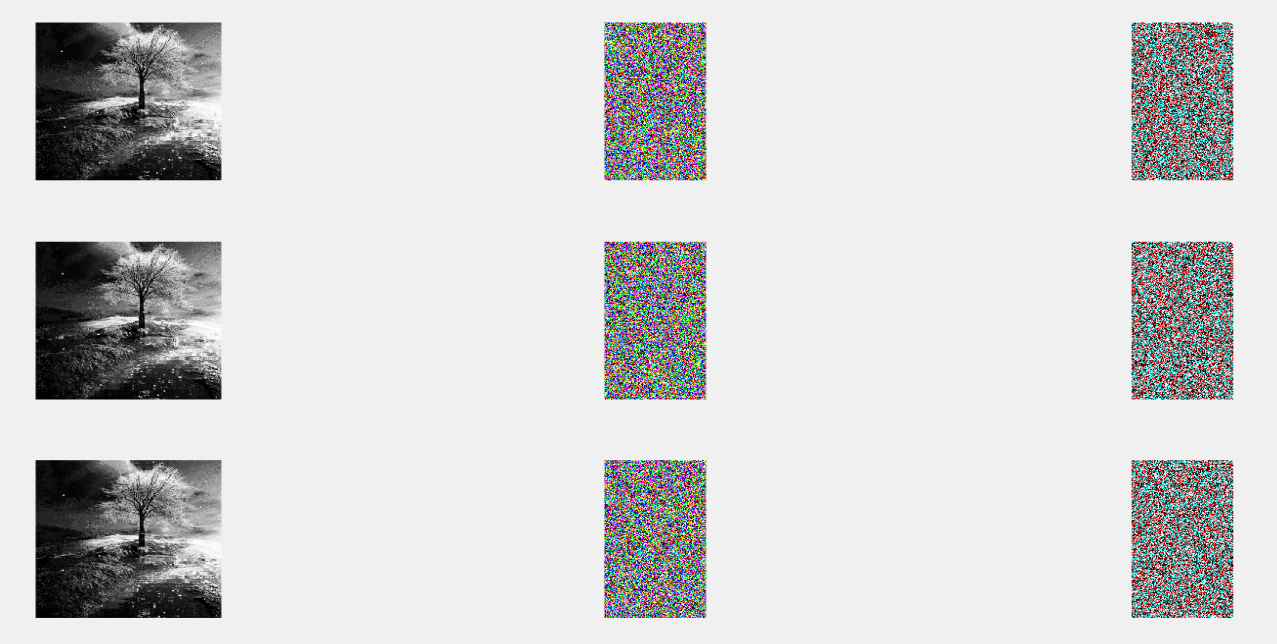

Fig. 6 three ciphered image of 3D images [12].

Table1: Time required for ciphering and deciphering 3D images

Image size	Type of image	Total time required for cipher	Total Time required for decipher	Number of multiple images	Total time for ciphering 3D image	Total time for Deciphering 3D image
4096X4096	Gray	613 msec	608 msec	20	~ 12.432 s	~12.042 s
2560x2560		254 msec	259 msec	33	~ 8.93	~ 9.003
2304x2304		169.2 msec	166.3 msec	29	~ 4.89	~4.773
4096X4096	Color	1.952	1.852	29	~56.608	~56.718
2560x2560		756 msec	767 msec	21	~15.37 sec	~15.221 sec
2304x2304		550.535 msec	553.121 msec	28	~15.534	~15.239

III. CONCLUSION

The cyber attack is increase day after day and the data that usage over the internet is increased day after day. The way of protecting the privacy of the data is by finding best and rapid cipher techniques to cryptography the data. The TEA is one of the best ciphered techniques and have the capability to ciphering high Image that contain high resources data such as 3D images with minimum time. The dividing the images into 8 pixels when ciphered helps to rapid the process of ciphering by eight times. The next steps for this project are to cipher video graphic and to used it on FPGA or Raspberry Pi device to test the capability of the TEA on performing in low cost processer.

REFERENCES

[1] Guard., "The Importance of True Randomness in Cryptography," whitepaper, 2017, 2017.

[2] A. A. Al-Hilali, L. Jumma, and I. Amory, "High-Quality Image Security Implementation Using 128-Bit Based on Advanced Encryption Standard algorithm," Journal of Southwest Jiaotong University, vol. 54, no. 6, pp. 1-8, 2019.

[3] A. Ç. B. Berna Örs, O. S. Kayhan and A. T. Erozan, "JPEG Image Encryption via TEA Algorithm," in 2015 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 2015.

[4] E. M. Galas and B. D. Gerardo, "Implementing Randomized Salt on Round Key for Corrected Block Tiny Encryption Algorithm (XXTEA)," in 2019 IEEE 11th International Conference on Communication Software and Networks, IEEE, 2019.

[5] Ü. K. S. Z. A. &. P. I. Çavuşoğlu, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," Nonlinear Dynamics, vol. 92, no. 4, pp. 1745-1759, 2016.

[6] E. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation: NIST Publishes SP 800-133 Revision 1," Information Technology Laboratory computer secuirty division, Unitied state, 2012.

[7] S. Balasubramanian, "Image encryption using infinite series convergence," in 18th International Conference on Systems Engineering (ICSEng'05), Las Vegas, NV, USA, USA, 2005.

[8] K. Marton, A. Suciu, Ignat and Iosif,, "Randomness in Digital Cryptography: A Survey," Romanian Journal of Information Science and Technology, vol. 13, no. 3, pp. 219-240, 2010.

[9] R. M. S. H. N. &. A. T. Ueno, "A high throughput/gate AES hardware architecture by compressing encryption and decryption datapaths," in In International conference on cryptographic hardware and embedded systems, Berlin, 2016.

[10] A. Mitra, Y. V. Subba Rao and S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques," International Journal of Computer Science, vol. 1, no. 2, pp. 127-131, 2006.

[11] S. M. H. e. al, "Security of Image File with Tiny Encryption Algorithm And Modified," Journal of Physics: Conference Series, vol. 1566 , no. 012108, pp. 1-7, 2020.

[12] "googleusercontent," [Online]. Available: https://lh3.googleusercontent.com/proxy/EBx3wZbsZPK9Za0cF08nprgCFO9rGrYYWfehkpgYcbBFcEAE9ou7k_FNOztWZtNWuLIzj6BKv0qOaZCASFqX2omD2uKC_7W0mW_H1f. [Accessed 17 11 2020].

[13] "cdn.nextgov.com," [Online]. Available: https://cdn.nextgov.com/media/img/upload/2019/09/10/shutterstock_767544493/route-fifty-lead-image.jpg. [Accessed 17 11 2020].