International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2021.3684

E-ISSN : 2454-6135

Volume.7, Issue 1
January -2021

Image Encryption based on a New Generation of Key from Rubik's Cube Principle of AES Algorithm

Raghda Sattar Jabar[1], Iman Hussein AL-Qinani [2], and Zainab Khyioon Abdalrdha [3]

[1]Assistant Teacher, [2,3]Teacher

[1] Department of Quality Assurance and University Performant, Mustansiriyah University, Baghdad-Iraq

[2,3]Department of Computer Science, College of Education, Mustansiriyah University, Bagdad-Iraq

ABSTRACT

Encryption is the most secure way to save data, whether text, images, video, or any other type of multimedia, as in recent years, a lot of encryption algorithms have been suggested to protect this digital data from all kinds of attacks, and the protection process was carried out through encryption and the use of many algorithms. Through the proposed method, this research was focused on an important aspect, which is protecting the key by creating a new method for the algorithm key, as the more difficult it is to know the key, the more difficult it is to break the algorithm, as Rubik's Cube method was used to create the key of the AES algorithm, where it performs just throw the cube to generate the key, then the improved algorithm was used to encrypt the images and then restore the original image without problems and the process was of a high quality as the key configuration time was reduced and a good level of security was provided. The proposed method has been programmed in Visual Basic.Net 2015 language.

Key Words: *Encryption, Advanced Encryption Standard (AES), Image Encryption, Rubik's Cube& key generation.*

1. INTRODUCTION

Due to the rapid advancement in technology in recent years; it has increased the portability of digital images, which can be easily found online. Therefore, the solution to the preservation of the image data is to encrypt it, as these images have their role in most medical or military applications or various multimedia systems [1]. Cryptology is an important science that transforms data into incomprehensible data so that it cannot be read (encrypted text), depending on an encryption key, and the obverse way is decryption where the incomprehensible text can be retrieved into a clear, readable text depending on the same key [2]. The encryption process depends primarily on the key used. Hard-to-guess knowledge of the key was difficult to crack the algorithm, so the cipher was split into two categories; symmetric key cipher, and asymmetric key cipher [1, 3]. In symmetric encryption algorithm, which is known as a private key, it is used one key for both encryption and decryption process [3]. In the asymmetric algorithm, which is also known as general encryption, it is used two keys, one key for encryption process of and the other key for decryption process [3]. Symmetric algorithms are quicker than asymmetric algorithms like AES, DES, Triple DES, etc. Therefore, symmetric algorithms are widely used [1, 3]. This paper will provide a brief overview of each of the AES algorithm and the Rubik's Cube that was used to generate the keys of the AES algorithm, in addition to describing the architecture of the proposed method and the way of its implementation in encoding and retrieving images and finally, it will describe the most important conclusions reached through the proposed method.

2. OVERVIEW OF ALGORITHM

Information systems that contain information, whether it is data from pictures or text or any other form of multimedia, where the process of securing it is an important process and requires great effort to provide it. Encryption is among the efforts that can be made to secure information systems, especially when it is transmitted over networks that consider insecure networks, for example, the Internet is insecure [4, 5]. Here, the most important algorithms are going to address which are followed in this research. As mentioned earlier, cryptography divided into two general categories depending on the algorithms used: Symmetric key and asymmetric encryption [1, 3, 5].

A. Rubik's Cube

In 1974, an architecture professor and sculptor invented a puzzle which is three dimensions named Rubik's Cube. It has been registered within the top 100 inventions of the 20th century in the United Kingdom, France and the United States, due to its unique properties that affected mankind. Technical personnel and scientists' interest have been attracted by The Rubik's Cube [6].

On the other side, furthermore, the Rubik's Cube architecture has many features that have been dealt with as physical models or tools such as rotation, switching, combinations, rotation, symmetry, and their purpose to study certain scientific cases or have been discussed using theory or scientific approaches in several fields. Scientists have begun to explore the principles of the internal movement of the Rubik's Cube architecture and the possibilities of applying Rubik's Cube have been explained depending on its rotational properties.

- **The Rubik's Cube origin**

Luo's Chinese book is one of the basics of constructing the concept of Rubik's Cube that could be represented in Jiugong map, as shown in figure 1. Jiugong map is a cube that has the third degree with a nildimensional space. The n-order magic square is a specific order created by a set of numbers 1,2, 3…, n^2 in n-order square, that gives us the total of the numbers in each row, column, and two diametrical lines n $(n^2 + 1)/2$. This is named a magic square constant. The magic square constant of the cube has the third degree is 15 [6].

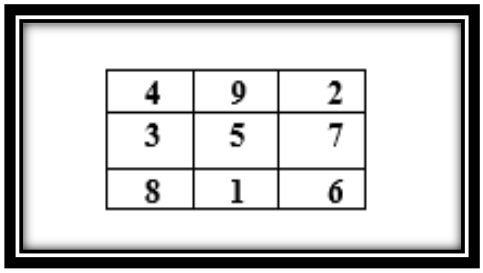

Figure 1: Jiugong map [6]

Jiugong Rearrangement, this type of cube is a cube that is of the third degree and one-dimensional, which was developed from the map of Jiu gong in the time of the Chinese Yuan Dynasty, where this game puts a new arrangement, which is eight pieces and is moved in nine places on the board. This is done by Move the pieces to generate another pattern, complete the change of Jiu gong order. Jiu gong rearranged and moved west to spread and the cube's evolution from arrangement to dimension. Evolution did not remain constant, but rather spread and transmitted as Chinese scientists in the Qing Dynasty came up with the idea of using digital blocks for 3D magic squares. Actually, this was a 3D prototype of a cube where Rubik designed a rotatable mechanical cube in 1974 because the 3D magic square did not rotate. As shown in figure 2 . Which set up the world's first three-order arrangement and here. The cube resembles a ball and is turned with shackles to achieve a specific rotation [6]. This work was carried out by Rubik, as shown in figure 3.

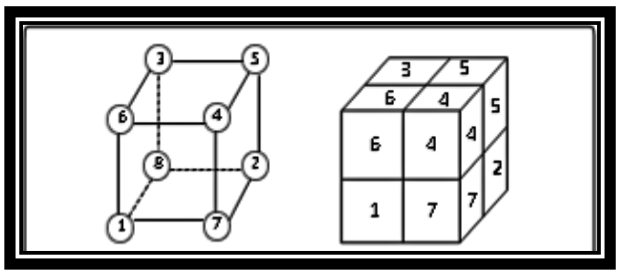

Figure 2: Rubik's Cube for a 3D prototype [6]

Figure 3: Mechanical rotating Rubik's Cube [6]

The cube can be designed or redesigned in such a way that it does not affect the rotation of the cube's body, and this is observed in figure 4. As the Chinese manufacturer Sheng Shou produced cubes of all sizes as of late 2013, the sizes ranged from 2 x 2 x 2 to 10 x 10 x 10. In figure 5, there are six instances of the specially designed cube, and the structural shape of the specially shaped cube has been varied, including the multi-faceted cube, the spherical cube, the tetrahedral cube, the mirror cube, the gear cube, etc. as shown in figure 6, which are six examples of specially shaped cubes, are the latest development of the Rubik's Cube [6].

DOI : 10.31695/IJERAT.2021.3684

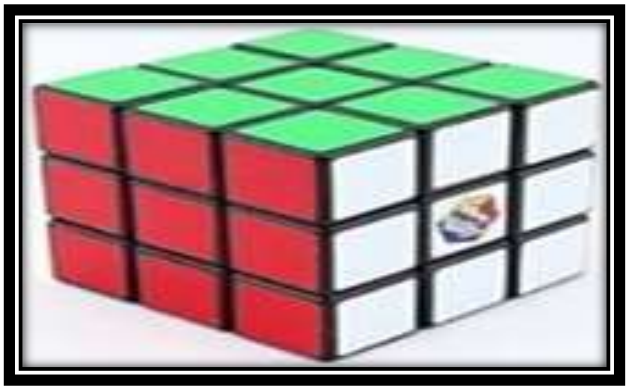

Figure 4: Current Rubik's Cube [6]

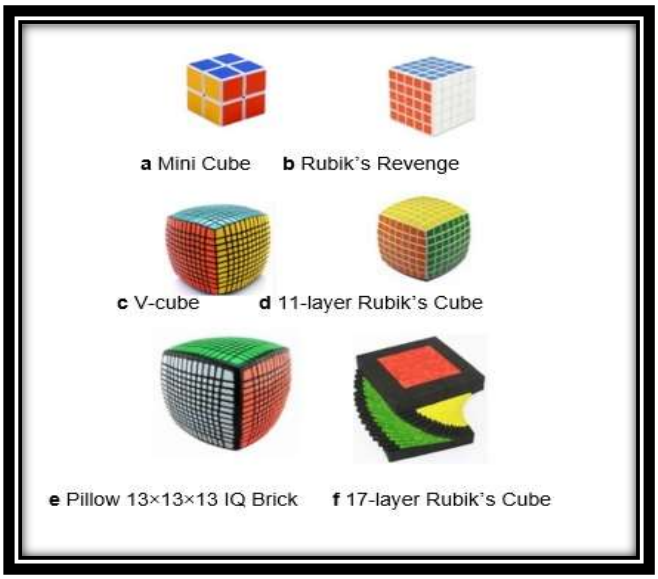

Figure 5: Models of Rubik's Cube [6]

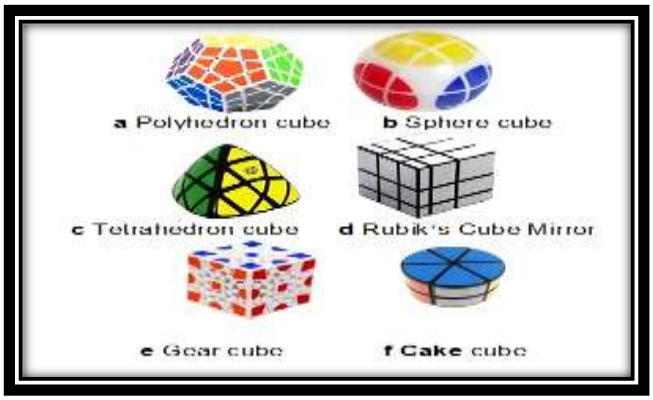

Figure 6: Specially Shaped Cubes [6]

In figure 7 it is shown that the Rubik's Cube consists of the number of faces that each one is able to go around its cube's core.

DOI : 10.31695/IJERAT.2021.3684

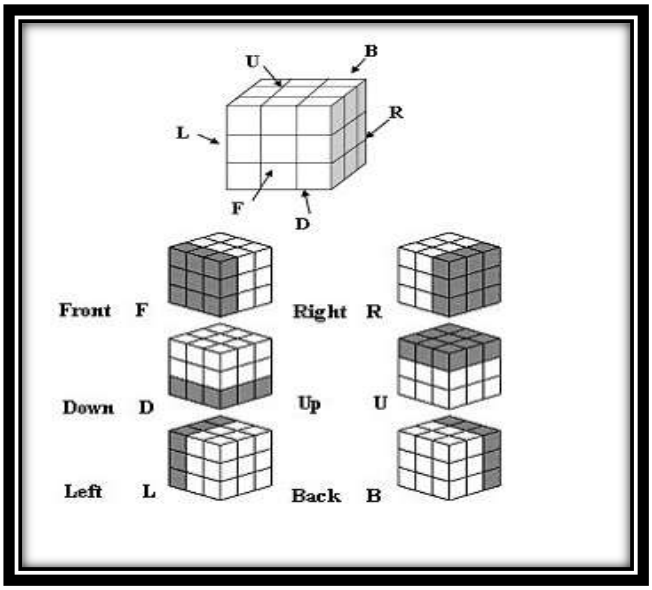

Figure 7: Rubik's Cube [6]

B. The Advanced Encryption Algorithm (AES):

It is one of the symmetric encryption algorithms that is characterized by speed and processing time due to its adoption of the same key in both encryption and decryption as a 128-bit key was generated which provided more security, performance, efficiency, and flexibility, is well suited to AES algorithm [7]. In addition to being more resistant to current attacks. The AES algorithm consists of 128 block length of bits that support other keys of length 11, 13, or 15 subkeys each of 128, 192 and 256 respectively [1, 3, 4, 7], and 128 bits each have one subkey that corresponds to each round of AES processing; Therefore, each subkey can be indicated to as a round key. Where is the Add Round Key phase, which combines using the XOR function, and the combination of the block of the current state data and the round key matching to the specified round, then the Sub Bytes phase replaces every byte through the fixed lookup table and inserted it into it, and that is between the case data while the four bytes of case data in every row are rotated the Shift Rows phase within an array the process of performing a quad-byte conversion of the case data in every column in the case data array is in the Mixed Columns phase[7]. The steps of the AES algorithm are stated in figure 8.

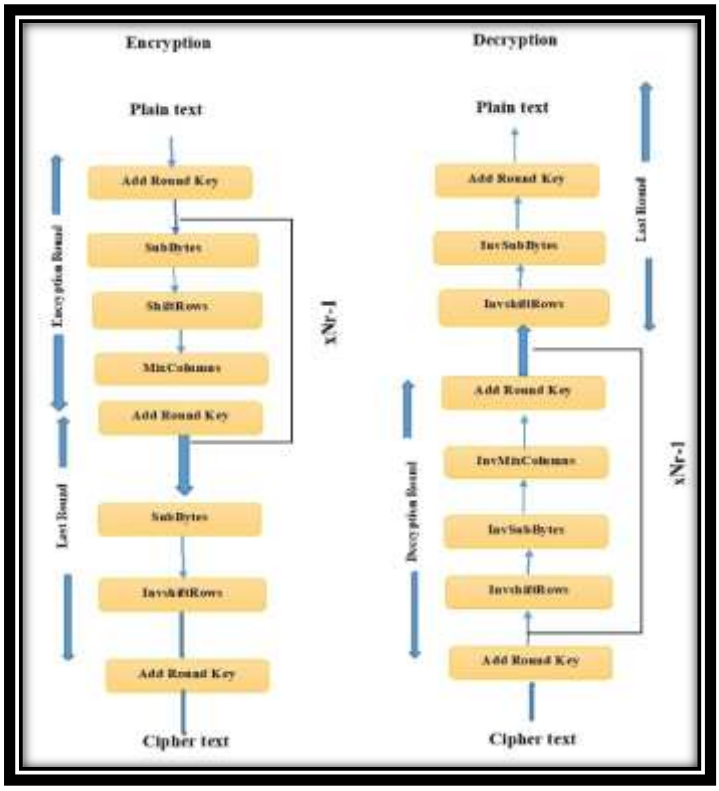

Figure 8: AES Encryption and decryption Process [7, 8, 9, 10]

DOI : 10.31695/IJERAT.2021.3684

3. GENERAL OUTLINE OF THE PROPOSED SYSTEM

In this part, architecture of the proposed method is going to be explained, which is the methodological framework that represents how to generate the AES algorithm key from Rubik's Cube and how to encode the color image based on the optimized algorithm and how to retrieve it as shown in figure 9, which represents a detailed diagram of the proposed method.

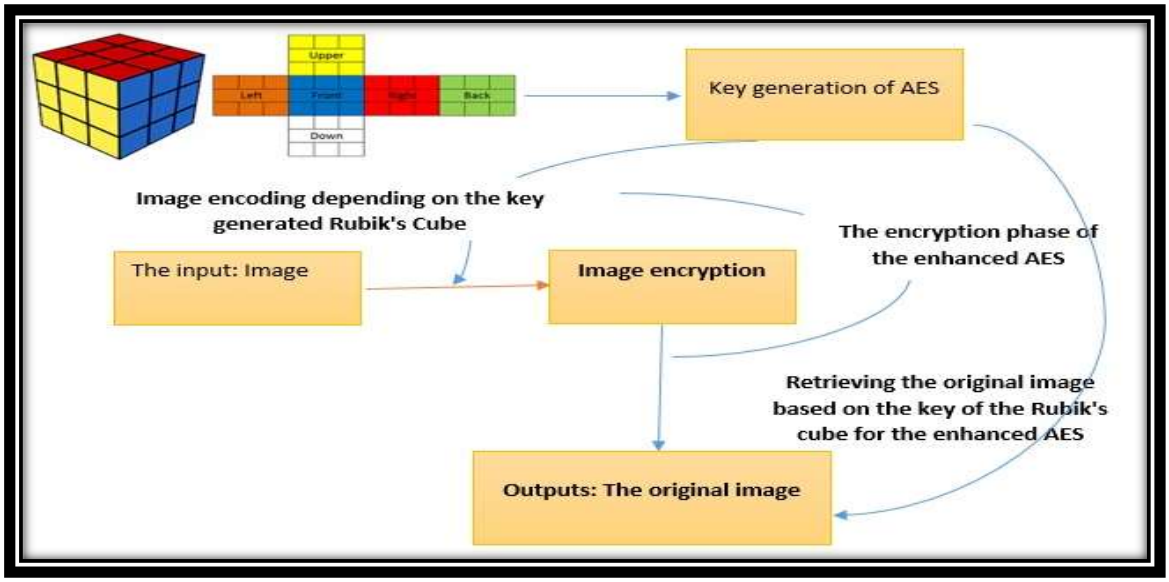

Figure 9: the outline of the proposed method

4. IMPLEMENTING THE PROPOSED METHOD

This part is going to explain the steps that were followed to apply the proposed method, which was represented by three stages, which are clarified in figure 10 that represents the steps involved to implement improved AES algorithm.

Input: Generate a key for an Image & original image for encryption

Output: Encrypted image

Step 1: Generate a key for the AES algorithm using Rubik's Cube that is generated a random key from the six sub-arrays on the six faces with one-sided cells being 16 face cells with dimensions (4 × 4) for a magic cube and the faces are (up (U), forward (F), right (R), Left (L), down (D), and backward (B).

Step 2: At the sender's side, upload the original image to be encrypted based on the key generated by the Rubik's Cube.

Step 3: Image encryption based on the improved AES algorithm whose keys were generated from the Rubik's Cube.

Step4: On the recipient side, the original image is retrieved depending on the improved AES algorithm whose keys were generated from the Rubik's cube, which is the decryption stage.

Step 5 :End.

Figure 10: Implementation steps for the proposed method

- **The Key Generation from the Hexagonal Rubik's Cube:**

The proposed method usually describes the cubic structure of a three-dimensional matrix. In this paper, the six sides of Rubik's Cube base are represented as it contains six faces, which are in the sequence (U) represents the top, (D) represents the bottom, (L) represents the left, and (R) represents the right and front (F), and behind (B). We used faces (4 × 4), the number of faces is (6), the number of cells formed in one face (96), and the length of the key (256) was established. Therefore, it is difficult

DOI : 10.31695/IJERAT.2021.3684

to guess this key by brute-force attacks because it is hard to arrange the cube which is impossible to anticipate by the attacker and to know or derive the key. As shown in figure 11, that was involved in the configuration of the proposed method of key generation.

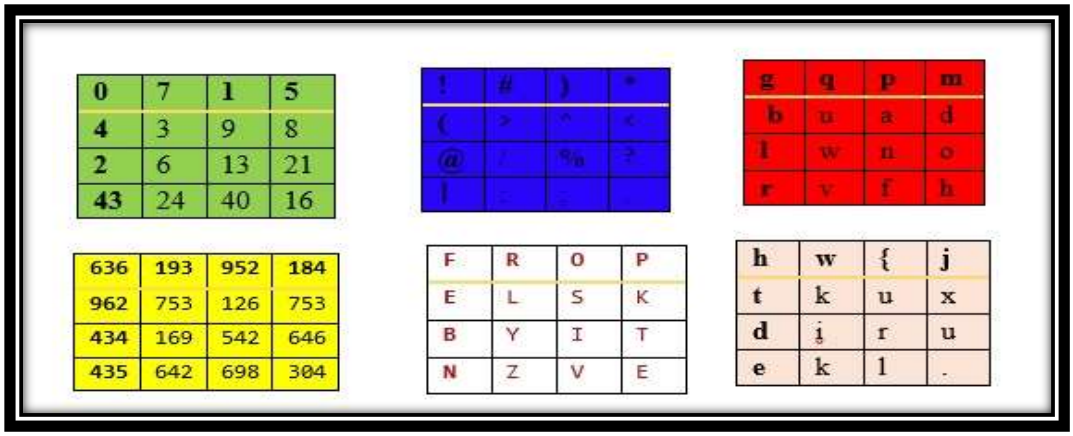

Figure 11: The proposed Rubik's Cube to generate a key algorithm AES

- **The Encryption Process**

The generated key from the Rubik's Cube was used to encode a color image, which in turn consists of 24 bits, as it includes red, green and blue. The resulting encryption logic works depending on the rest of the operations of the AES algorithm and the repetition of operations to reach the last process in encoding the image as shown in the application side of the associated method.

- **The Decryption Process**

This part indicates reversing the encoding process, but it requires knowledge and generation in the same way on the encoder side in order to retrieve the original image. Therefore, this is difficult for an attacker to detect the key or guess in the event that there is no information about the Rubik parameters used for the hexagonal face, where the mixing technique using Rubik's Cube and key generation for creating a random key that is hard to guess.

- **The Practical Aspect of the Proposed Method:**

This part is going to clarify implementing the proposed method in the application according to the steps described in figure 10 that showed how to generate the key for the AES algorithm from Rubik's cube, then encode and retrieve the original image according to the improved algorithm method. The interface of the proposed method is shown in figure 12.

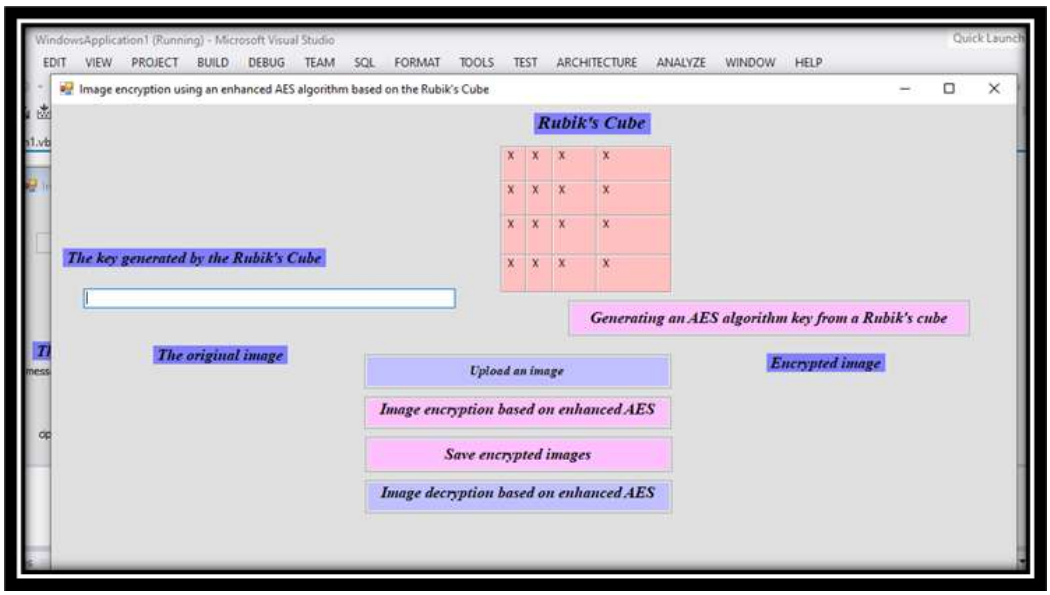

Figure 12: The interface of the proposed method

DOI : 10.31695/IJERAT.2021.3684

In the first step, the AES key is generated from the Rubik's Cube as in figure 13.

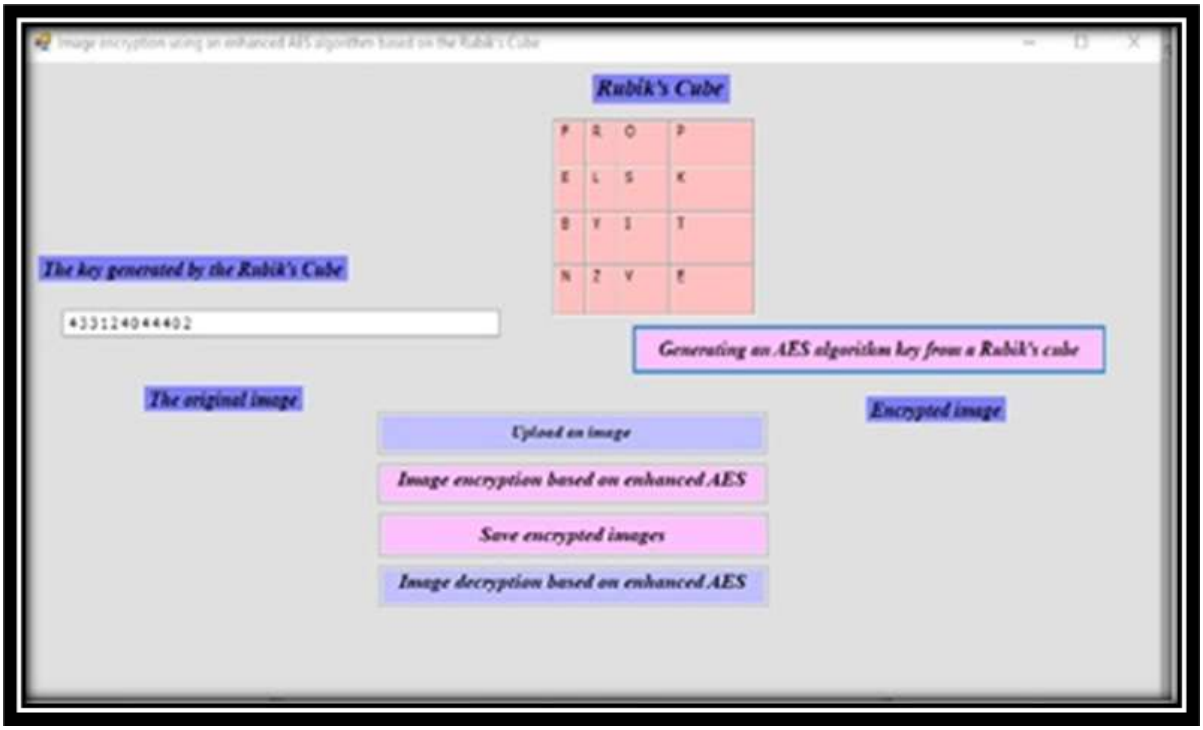

Figure 13: Generate the AES key from the Rubik's Cube

In the second step, the original image is uploaded as shown in figure 14, then encodes the image, and stores it as in figure15.

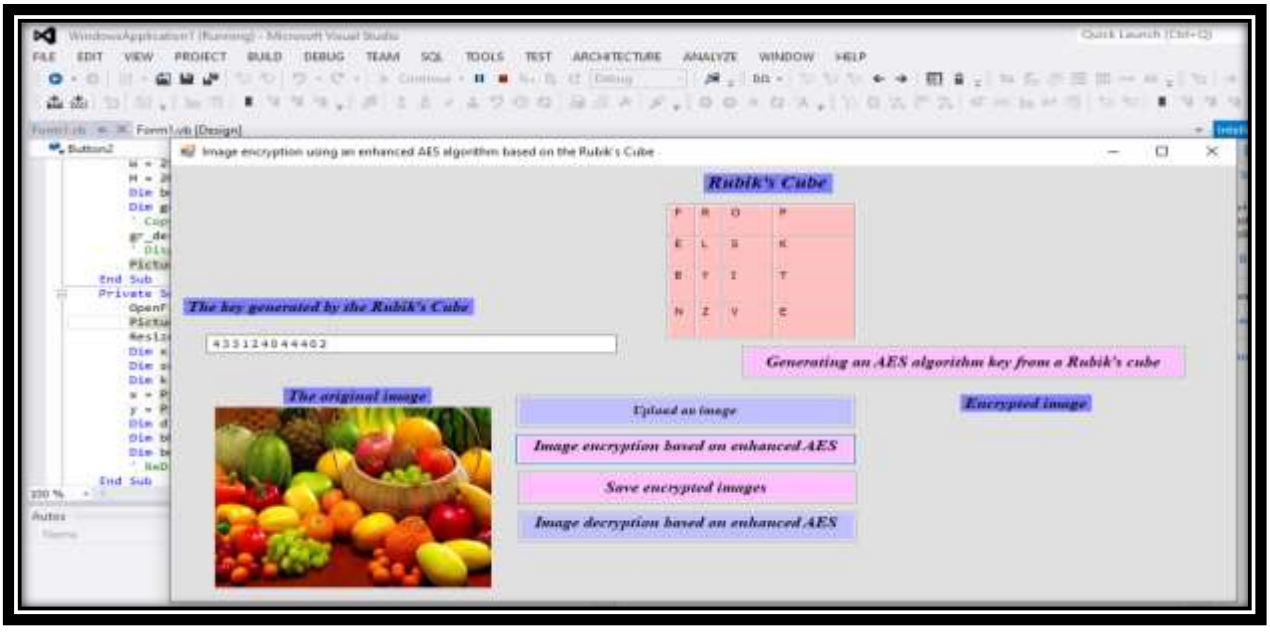

Figure 14: Upload the original image

DOI : 10.31695/IJERAT.2021.3684

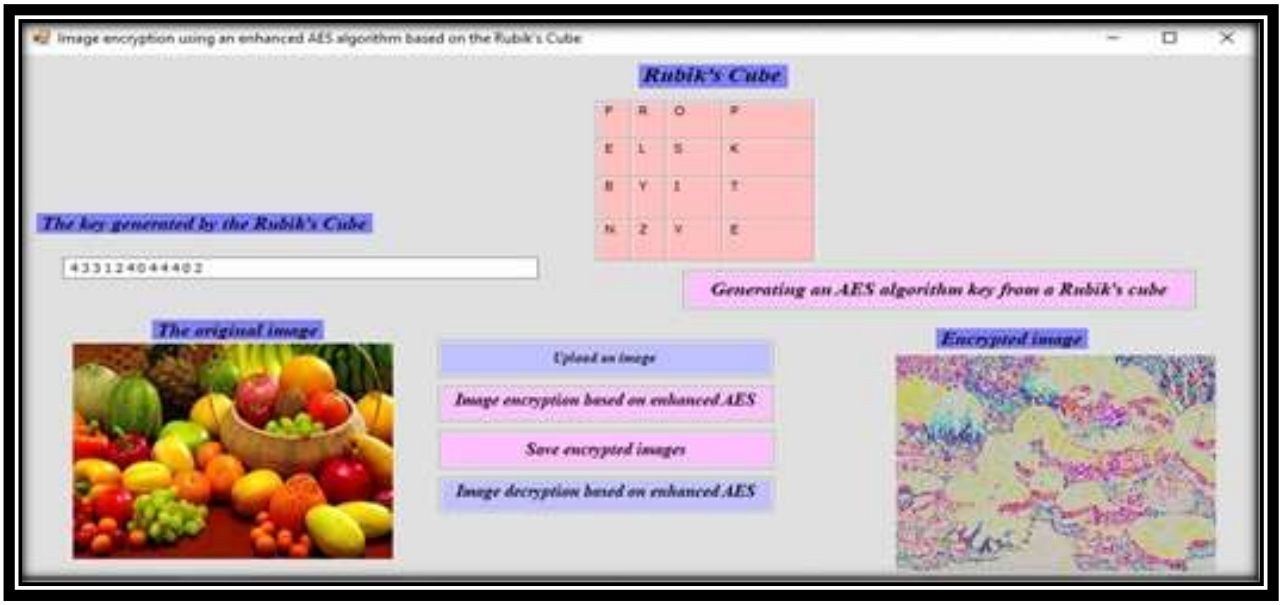

Figure 15: Image encryption based on enhanced AES algorithm

In the third step, the receiving side uploads the encrypted image, then decodes it, and retrieves the original image as shown in figure 16.

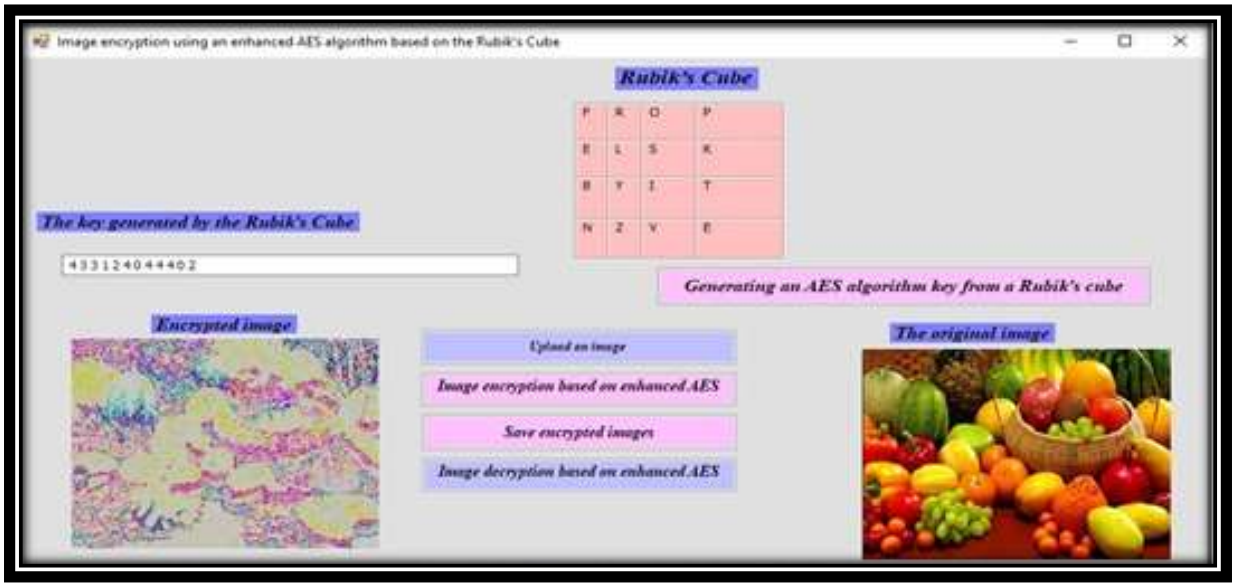

Figure 16: Retrieved of the original image

5. CONCLUSION

Image encryption is extremely important, especially in the medical, military, and other IT fields, so most websites and networks require the use of an algorithm with better performance and security for strong keys. The use of the improved algorithm in image encryption and the applying of the proposed method that demonstrates the speed of encryption, in addition to a newly proposed image encryption scheme which generated a random key from Rubik's Cube and can achieve good cryptography and can resist any analytical attacks. In the future, it is possible to apply a Rubik's Cube to asymmetric cryptographic algorithms. In addition, modifications can be added to the proposed method to include multiple media such as video, audio, etc.

ACKNOWLEDGMENT

The authors would like to thank Mustansiriyah University (www. uomustansiriyah.edu.iq) Baghdad - Iraq for its support in the present this work.

DOI : 10.31695/IJERAT.2021.3684

REFERENCES

[1] Alrababah, A. A., & Alrasheedi, M. (2017). Digital image encryption implementations based on AES algorithm. *VFAST Transactions on Computer Sciences, 5(1),* 09-17. https://vfast.org/journals/index.php/VTCS/index

[2] Chowdhury, R., & Ghosh, S. (2011). Normalizer based Encryption technique (NBET) using the proposed concept of Rubicryption. *International Journal of Information Technology and Knowledge Management*. 4(1), 77-80. https://www.csjournals.com/?p=39

[3] Seth, R. M., & Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication. *International Journal of Computer Science and Technology, 2(2),* 292-294. http://www.ijcst.com/

[4] Simarmata, J., Limbong, T., Ginting, M. BR., Damanik, R., Nasution, M. I. P., Hasugian, A. H., … Mesran, M. (2018). Implementation of AES algorithm for Information Security of Web-based application. *International Journal of Engineering & Technology*, 7 (3.4) 318-320. https://www.sciencepubco.com/index.php/ijet/index

[5] Singh, G., & Supriya (2013). A Study of Encryption algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications. 67(19),* 33-38. https://www.ijcaonline.org/archives/volume67/number19

[6] Zeng, DX., Li, M., Wang, J., Hou, Y., Lu, W., & Huang, Z. (2018). Overview of Rubik's Cube and reflections on its application in mechanism. *Chinese Journal of Mechanical Engineering*. 31(77),1-12. https://doi.org/10.1186/s10033-018-0269-7

[7] Priya, S. S. S., Karthigaikumar, P., & SivaMangai, N.M. (2015). Generation of 128-Bit Blended Key for AES algorithm. *In: Satapathy S., Govardhan A., Raju K., Mandal J. (eds) Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Advances in Intelligent Systems and Computing, vol 338. Springer, Cham*. https://doi.org/10.1007/978-3-319-13731-5_47

[8] Reddy, M. S., & Babu, Y. A. (2013). Evaluation of Microblaze and implementation of AES algorithm using Spartan-3e. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.2(7),* 3341-3347. http://www.ijareeie.com/volume-2-issue-7

[9] Acla, H. B., & Gerardo, B. (2019). Performance evaluation of lightweight advanced encryption standard hardware implementation. *International Journal of Recent Technology and Engineering. 8(2),*1810-1815. http://www.ijrte.org/download/volume-8-issue-2/

[10] Mulani, A. O., & Mane, P. B. (2015). High-Speed area-efficient implementation of AES algorithm on reconfigurable platform. *Sen, J. and Mehtab, S. (eds) Computer and Network Security, London, United Kingdom.* 119-140. DOI: 10.5772/intechopen.82434

DOI : 10.31695/IJERAT.2021.3684