Visual Cryptography Using RSA Algorithm and 2-bit rotation

[1]Varun C M, [2]Venu Dattathreya V, [3]Varshith Y, [4]Sunnihith Reddy I, [5]Nagendiran S

Assistant Professor, Department of Computer Science and Business Systems,
R.M.K Engineering College, Chennai, Tamil Nadu

Third Year, Department of Computer Science and Business Systems
R.M.K Engineering College, Chennai, Tamil Nadu
Third Year, Department of Computer Science and Business Systems,
R.M.K Engineering College, Chennai, Tamil Nadu
Computer Science and Business System,
R.M.K Engineering College,Chennai, Tamil Nadu
Assistant Professor, Department of Artificial Intelligence and Data Science
R.M.K Engineering College,Chennai, Tamil Nadu

cmvarun87@gmail.com, venudattathreya@gmail.com, varshithyadavalli@gmail.com , sunnyreddy0981@gmail.com, nagendiransubburaj@gmail.com

Abstract - The field of information security is fascinating, and image encryption is no exception. With the help of cryptography, information can be using a 1-bit rotation by RSA. transmitted secretly. Although in a different approach, this technique similarly aims to preserve information. Due to its characteristics, encrypting an image is different from encrypting text. There are numerous algorithms for this operation. Numerous algorithms are used in cryptography, including RSA, IDEA, AES, and DES; however, in this case, we only utilize RSA because it is sufficient to carry out a combined procedure using 2-bit rotation. The goal of this project is to use the RSA algorithm to encrypt photographs. The encrypted image is accepted by the network as input for additional processing. Images are encrypted With a 1-bit rotation, just one bit is changed, and the shifted bits are reversed on the decrypting side. To increase security, we will instead use a 2-bit rotation, which is more secure than the current method. The image is permuted to create an encrypted image after the 2-bit rotation. To work with RGB picture encryption, the RSA method was changed. According to test results, the proposed method can successfully encrypt and decrypt a variety of images, and the algorithm has robust encryption properties. By using this technique, a cipher image that is distinct from the original image will be created. The safe transmission of photographs over the Internet is made possible by this technology's enhanced security.

Keywords- *RSA Algorithm, Images, 2-bit Rotation, Ciphe*

I.INTRODUCTION

There is a method being used right now to transmit information secretly. Cryptography is the process by which this is accomplished. The method is frequently employed to safeguard data or information. Only the intended recipient will be able to decipher texts that have been encrypted. In this project, we'll create a brand-new system that uses an image that's been encrypted with the RSA and 2-bit rotation methods. to increase trust and security. RSA is a very secure cryptographic algorithm. In terms of confidentiality, data is encrypted using cryptography to prevent unauthorized access while it is stored on storage devices or sent across communication channels. Encryption is also used to protect the process of authenticating various parties who wish to use the system's features. Because a user who requests access to a certain function on the system must provide proof that they are who they say they are. It is important to take extra measures to make sure that only the rightful owner of that item—often referred to as credentials—uses it. The most popular and obvious credentials are passwords. To prevent unauthorized use, passwords are encrypted. To safeguard passwords for email accounts, Internet banking accounts, and other digital media, text protection is necessary. Given how frequently images are used in various operations, especially those online, safeguarding picture data from unauthorized access is essential. Image cryptography is a special kind of encryption that uses a key value to encrypt and decrypt the original message by hiding data within an image. Computational hardness is a rare property of algorithms, making it challenging to decipher the code and restore the original image. In industrial and scientific activities, image protection is necessary both during the transmission of images and their storage. The RSA encryption and authentication system was invented in 1977 by Leonard Adleman, Adi Shamir, and Ron Rivest. A public key cryptosystem, or cryptosystem, is RSA. To convey secure data, RSA is frequently utilized. To make the data unreadable before it is delivered, this technology will encrypt the data. Only

users who have the proper authorization will be able to accurately decrypt the data.

II.PROBLEM STATEMENT

The main objective of this project is to encrypt photos with the RSA algorithm and 2-bit rotation. However, in our project, we generate random values to compute the process, and the image size is converted into values by graph charting. In the classic RSA technique, the sender provides two fixed integer values to calculate the process. We construct the private key values using the RSA algorithm once the image has been plotted in a graph with the correct image height and width values. The numbers are turned into an RGB-encrypted image after being bit-rotated. The aforementioned algorithm is being used for military operations. We can use this procedure to transmit private image data to various defense cadets through a channel.

III. PROJECT SCOPE AND OBJECTIVE

The program's main goal is to protect sensitive image data because it is intended for military use. Security is the top concern to prevent data leaks. The RSA algorithm combined with a 2-bit rotation is used to encrypt and decrypt the image data. Contrary to text messages, multimedia data, especially image data, has distinctive characteristics, including redundancy and significant pixel correlation.

Security is one of the main requirements that must be addressed when transmitting information across a network. With the help of this technology, the data will be encrypted and transferred in an unreadable manner, making it possible for only authorized users to correctly recover the data.

Our project's main goal is to secure the image data.

- Encryption is used to convert the image to a cipher image using the public key.
- The private key is utilized in decryption to transform the cypher image to an image.
- To distribute classified image data to several military bases via a channel.
- Then, using the RSA system, we change the image to an encrypted image and the decrypted image.

IV. LITERATURE REVIEW

Literature review on image encryption and decryption using RSA algorithm and 2-bit rotation:

In a work released by Radhakrishna M, the authors attempt to encrypt and decrypt images based on the RSA technique while also offering authentication and using image hash functions for added security.

A picture encryption technique employing the RSA algorithm and a random image as a key is suggested in a different study written by Aradhana Sahoo, Pratyasha Mohanty, and Purna Chandra Sethi. The proposed method offers superior encryption quality than the alternatives, according to a comparison with various encryption techniques.

In a work, authors Raza Imam, Qazi Mhammad Areed, Abdulrahaman Alturki, and Faisal Anwer provide an organized and critical assessment of RSA-based public key cryptography systems. The study contrasts RSA techniques using many criteria, including key generation, encryption, decryption, key characteristics, and others.

In a publication, authors Dalia Mubarak Alsaffar, Atheer Sultan Almutiri, and Bashaier Alqahtani propose an investigation into image encryption based on the AES and RSA algorithms. Utilizing MATLAB, the study compares these two encryption techniques for image encryption.

Dr. Ganesh D. presents a chapter on the literature review that summarises prior research on the RSA algorithm that has been done in the realm of public key cryptography.

In a publication, Yaohui Sheng, Jinqing Li, Xiaoqiang Di, Xusheng Li, and Rui Xu propose a multi-directional diffusion-based complex network scrambling-based picture encryption technique. The key associated with plaintext is encrypted by the algorithm using the RSA algorithm, and an image-scrambling technique based on a complicated network is created.

These studies' suggested solutions use the RSA algorithm along with other methods like multi-directional diffusion and complicated network scrambling to increase the security and effectiveness of picture encryption schemes. These techniques can be applied in several situations where secure image communication is necessary.

V. PROJECT SPECIFICATION

PROPOSED SYSTEM:

A picture has been used as information in place of text or numbers in our suggested system, and a different image will be generated using the RSA algorithm's implementation key. The proposed algorithm's steps are as follows:

1. Consider the image and find out the array format.
2. Finding the length of an array.
3. Consider the key image and find out the corresponding

array format.

4. From the key image, any random prime number will be considered as key (For simplicity, we have considered any prime number as key among the key image array).
5. 2-bit rotation is also used to rotate the random numbers or pixel values of the image with 2-bit.
6. Then, the same key generation, encryption, decryption process can be done as the traditional one.

Advantages:

- System generates the random prime numbers for p, q variables.
- 2-bit rotation is also used to rotate the random numbers or pixel values of the image with 2-bit.
- It also converts RGB image to encrypted image. More secure and fast than the existing system.

Image cryptography operates according to the flowchart in Fig. 1. The encryption and decryption processing is broken down step by step in Fig. 1.

VI. MODULE DESCRIPTION

RSA:

A popular encryption algorithm that guarantees secure communication is RSA. A public key is used for encryption, and a private key is used for decryption. The security of the method is predicated on how challenging it is to factor in huge numbers. RSA has proven crucial in safeguarding sensitive data and securing digital communication.

The RSA algorithm, at its heart, achieves security through the use of modular arithmetic and the mathematical features of huge prime numbers. It is predicated on the idea that factoring huge composite numbers into their prime elements is computationally challenging.

Two keys are used by RSA: a public key and a private key. Anyone who wants to send an encrypted communication to the holder of the private key should provide the public key.

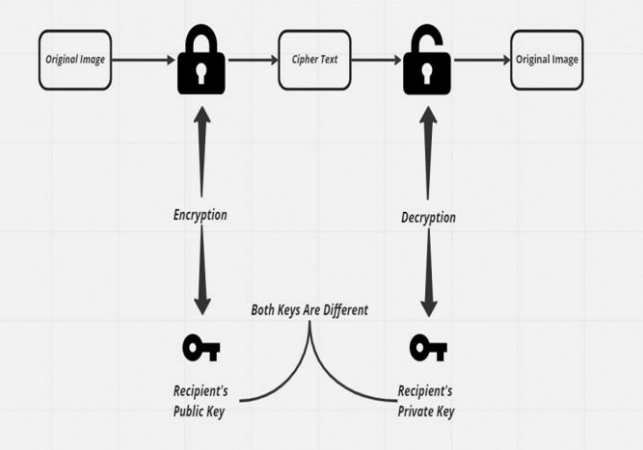


Fig. 2 RSA Diagram

The recipient uses the private key to decrypt the encrypted message, which must be kept secret.

Large numbers are challenging to factor, which is RSA's strength and the basis for its security. Longer key lengths are needed to maintain the same level of security as computational power rises.

All things considered, the RSA algorithm has been crucial in protecting digital communication, guaranteeing the secrecy and integrity of data, and laying the groundwork for several security protocols and applications. RSA algorithm process in fig. 2

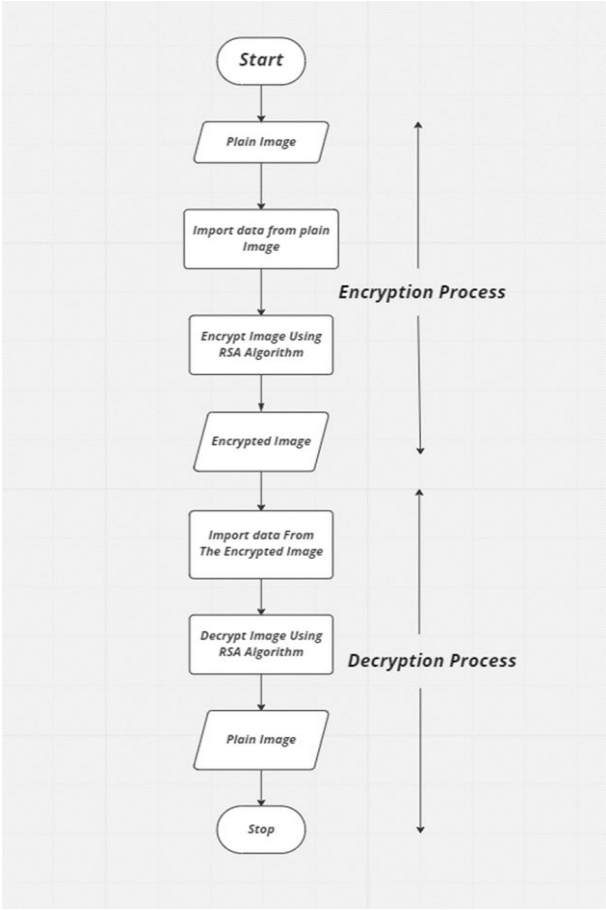


Fig no-1 Flow chart

Why is the RSA Algorithm used?

RSA offers an encryption method that makes sure that only those with the proper authorization may access and decipher the data

Encrypting data during transmission enables secure communication through insecure channels, such as the Internet.

Information secrecy is ensured by RSA, which stops unauthorized people from intercepting and deciphering the data.

RSA makes authentication easier by utilizing digital signatures. These signatures ensure that the sender is genuine and honest and that the message hasn't been tampered with.

Secure key exchange is made possible by RSA for two parties. It makes it possible for symmetric encryption keys to be distributed securely so they can be utilized for quicker and more effective encryption.

RSA is used for encryption, authentication, and key exchange in many secure protocols, including SSL/TLS for secure web communication, which guarantees secure online transactions.

ENCRYPTION

The process of converting data into unintelligible data that is not in its original format is known as encryption. It is necessary to encrypt data in order to secure it from assault and ensure that it cannot be reconfigured into its original form even if attackers steal the shares. In this project, we use two encryption algorithms: Caesar Cipher, a straightforward symmetric algorithm that adds each pixel's value to a fixed value (key), modifies the result by 256 because each pixel's value falls between 0 and 255, and RSA, a more robust algorithm that utilises two pairs of keys. To considerably boost security, two encryption methods are used.

DECRYPTION

The reconstructed image is decrypted by this module. First, the rebuilt picture is decrypted using the RSA algorithm. With the use of a key and Caesar cipher, the outcome is then decoded. These keys need to be connected to or identical to the ones used for encryption. If the wrong key is used, the original image will not be returned, and the secret will not be properly revealed. The use of the decryption techniques must be done in the right sequence. The Caesar Cipher algorithm should be used first when decrypting a picture because it was first encrypted using Caesar Cipher and then with RSA. The reconstructed image is decrypted by this module. Initially, the rebuilt picture is decrypted using the RSA method.If the encryption and decryption steps are not carried out in exactly the opposite sequence, the final picture won't be a perfect replica of the original. Additionally, in order to produce a legitimate image in the end, the keys used to decode the image must be 100% accurate.

VII. RSA ALGORITHM

There are three main encryption and decoding processes in the RSA algorithm. The steps are as follows:
1) Key Generation
2) The use of encryption
3) Decryption

Key generation
The RSA algorithm's key creation process comes first. Public and private keys are used in the RSA algorithm. The public key associated with those keys is used to encrypt messages and is publicly available. With the help of the private key, messages that have been encrypted with the public key may be decoded. The following processes produce the RSA algorithm's keys:

· Choose p and q so that they are both p,q prime numbers, p≠q.
· n=p×q
· q(n) = (p-1) (q-1)
· Select an integer e such that : g(d ((n), e)) =1 & 1< e < (n)
· de = 1 mod (q(n))
· PU= {e, n}
· PR ={d,n}

B. Encryption

In order to ensure that gcd(m, n) = 1, first convert M into an integer. The cipher text c is then calculated.

· Plaintext : M
· Ciphertext: C = (M^e) mod n

C. Decryption

· Ciphertext: C
· Plaintext : M= (C^d) mod n
· Note 1 : (n) -> Euler's totient function
· Note 2: Relationship between C and d is expressed as:
ed (mod (n)) =1
ed = 1 mod (n)
d =e−1 mod (n)

2-bit Rotation Process:

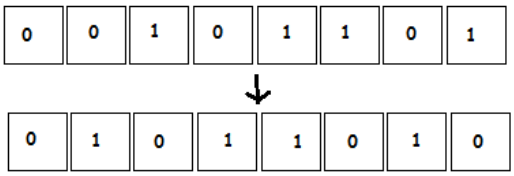
In 2-bit rotation, the image's pixel values, or random integers, are rotated using two bits. We first choose the

image's size, after which we create the key using the pixel values of the image. The key value should then be converted to binary format before being rotated by two bits. The 2-bit key is rotated or shifted in this step. This strategy will help secure our reputation.

1 bit leftward rotation:

Consider the case where we want to left-rotate the 16-bit position of the integer (n) by one bit (d). As can be seen in the example below, shifting happens after the number is encoded in 8 bits as 00010000. When the number is shifted, the outcome is 00100000, which, when expressed in decimal form, is 64. As a result, when a number is moved to the left, the following outcome occurs:

$$l = n * (2^d)$$

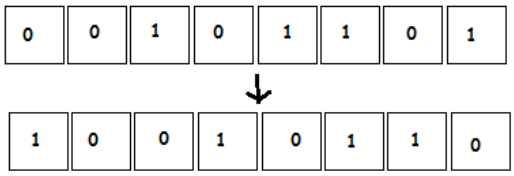


LEFT SHIFT EXAMPLE

1 bit of rightward rotation

$$r = n / (2^d)$$

IX.TESTING



RIGHT ROTATION EXAMPLE

VIII. APPLICATIONS OF IMAGE CRYPTOGRAPHY

Under the direction of core banking, a networked group of bank branches provides a number of services. Customers of the bank can conduct quick transactions and access their funds at the member branch locations. The key issue in core banking is the validity of the consumer. Due to the inescapable hacking of online databases, it is always exceedingly challenging to trust the information found there. The authentication problem is addressed by a suggested technique based on image processing and image cryptography. The popularity of online multimedia apps is rising. While being stored and sent across a network, the valuable multimedia content, like the photograph, is open to unauthorised access. Forensics, robotics, and military communication are just a few industries that frequently use image processing.

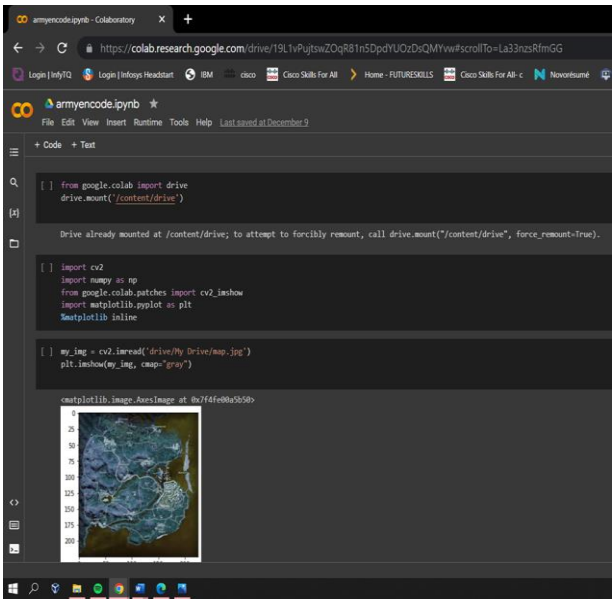


Fig.3 Testing

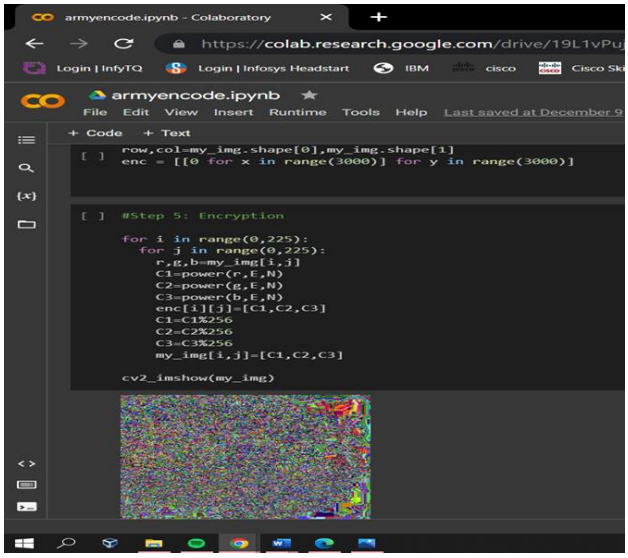


Fig.4 Testing Encryption Sample

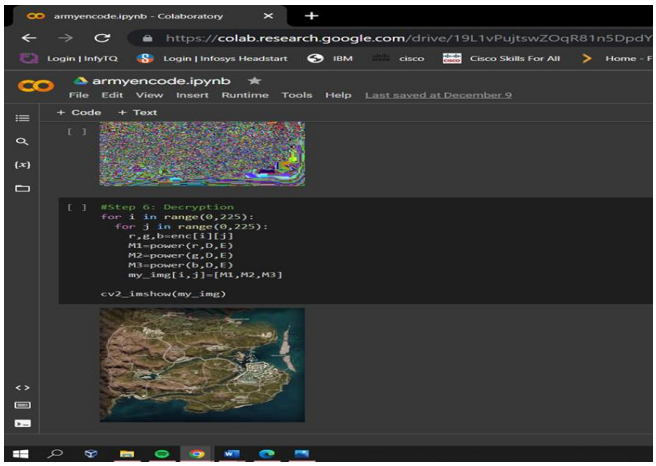


Fig.5 Testing Decryption sample

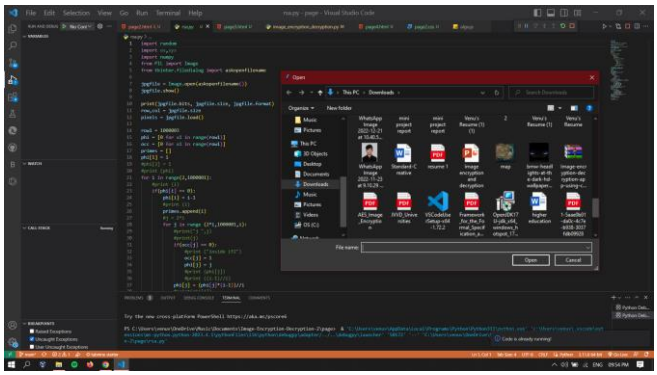


Fig.6 Choosing the image

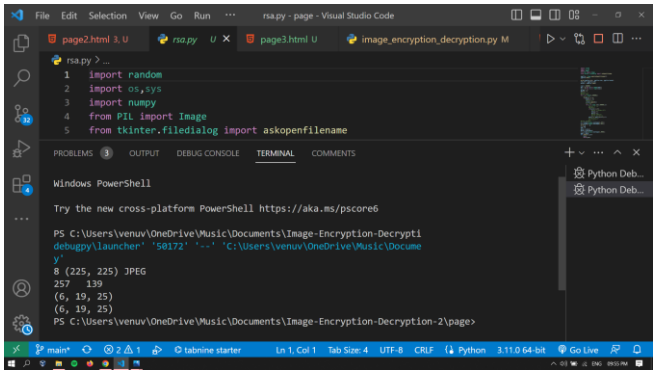


Fig.7 Rgb values

X. RESULT AND DISCUSSION

To test this, multiple raw photos of various sizes are encrypted and decoded. In this study, 2-bit rotation encryption and the RSA method are used to boost the security of the encrypted data. In this case, one key is required to encrypt the picture, and a different key is required to decode it. Finally, the experiment on picture encryption and decryption shows that it is possible to secure images on networks.

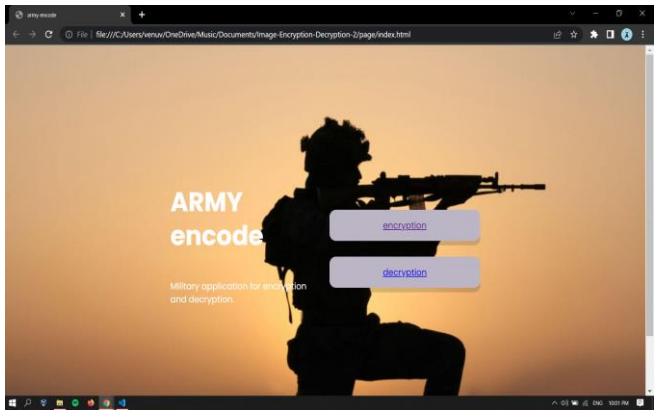


Fig.8 Home page

Fig.9 Encryption page

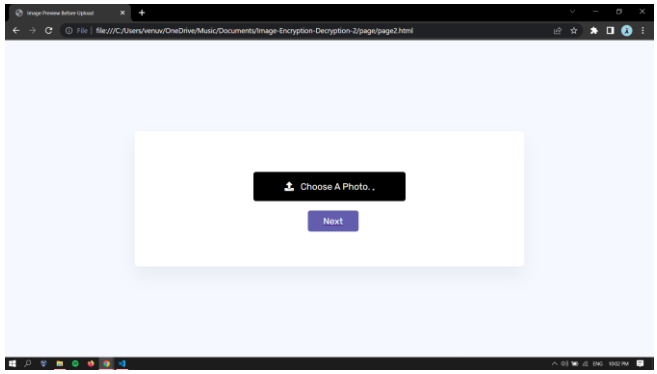


Fig.10 choose image

As an original image could include the data, the image contains a secret and will be encrypted. It is depicted in Fig. 11.

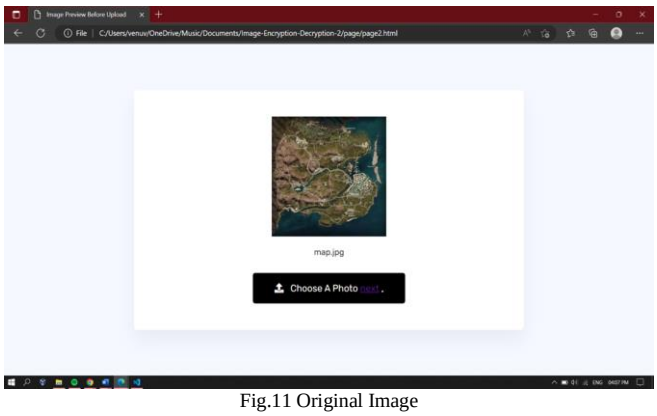


Fig.11 Original Image

The key produced by the RSA technique encrypts the original picture. The cipher text is being created from the picture. It is seen in Fig. 12.

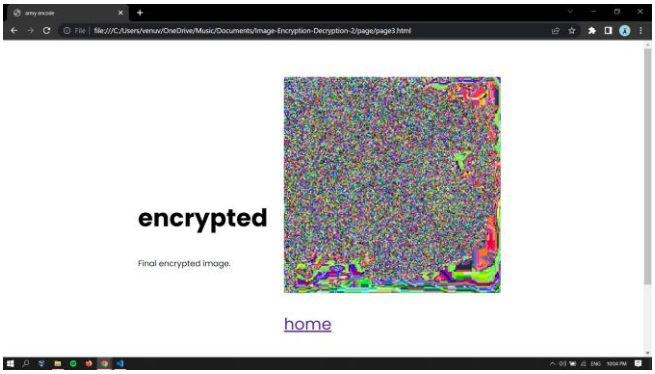


Fig.12 Encrypted

By using a second decrypt key that is likewise produced by the RSA technique, the cipher text is finally decoded. Additionally, it creates the final picture from the cipher text.

XI. CONCLUSION

Photo security has taken on increased significance since communication has expanded quickly in the digital age.

It is now suggested to use a picture as the key.

• According to the study's conclusions, the algorithm has advantages based on the various techniques applied to data photos.
• There is no data loss because the decrypted picture perfectly matches the original image.
• The performance study of the suggested method is 40% better than using text as a key. Without the secret key, it is impossible to determine the original picture.
• Therefore, it was shown that the various strategies applied here are efficient for encrypting photos using the images as keys and that they offer greater security on an open network.

XII. REFERENCES

[1] Kalyan Chakraborty, "Introduction to Basic Cryptography", CIMPA School of Number Theory in Cryptography and Its Applications School of Science, Kathmandu University, Dhulikhel, Nepal July 20, 2010.

[2] Vishwagupta, Gajendra Singh ,Ravindra Gupta," Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[3] Shikha Kuchhal, Ishank Kuchhal," Data Security Using RSA Algorithm In Matlab", International Journal of Innovative Research & Development, Volume 2,Issue 7, July 2013 ISSN:2278-0211(ONLINE).

[4] Abdul D S, Eliminaam ,Kadar H M A and Hadhoud M M (2008), " Performance Evaluation of symmetric Encryption Algorithms," IJCSNS International Journal of Computer Science and Network Security , VOL.8 No. 12,December.

[5] Gurjeevan singh, Ashwani single, K S sandha,"cryptography algorithm comparison for security enhancement in wireless intusion detection system, "international journal of multidisciplinary research, vol .1 issues 4, august 2011.

[6] A.Nadeem, "A performance comparison of data encryption algorithms", IEEE information and communication technologies, 2006.

[7] Neeta settia,"Cryptanalysis of modern Cryptography Algorithms" .In IJCST.2010.

[8] Schneier, B. (1996), "Applied Cryptography", Wiley & Sons, p.399.

[9] Monika Agrawal "A Comparative Survey on Symmetric Key Encryption Techniques" In International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012.

[10] Mohit Marwaha, Rajeev Bedi, Amritpal Singh, Tejinder Singh "comparative analysis of cryptographic algorithms" International Journal of Advanced Engineering Technology "/ IV/III/July-Sept., 2013/16-18.

[11] Idrizi, Florim,Dalipi, Fisnik & Rustemi , Ejup. "Analyzing the speed of combined cryptographyic algorithms with secret and public key" .International Journal of Engineering Research and Development,e-ISSN: 2278-067X, p-ISSN: 2278-800X,www.ijerd.com Volume 8,Issue 2 (August 2013), pp.45

[12] Prashanti.G, Deepthi .S & Sandhya Rai.K. "A Novel Approach for Data Encryption Standard Algorithm ". International Journal of Engineering and Advanced Technology (IJEAT) ISS: 2249-8958, Volume -2 Issue-5, June 2013, pp.264.

[13] Vishwa Gupta, Gajendra Singh, Ravindra Gupta."Advance Cryptography algorithm for improving data security "International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Volume 2, Issue 1,January 2012 .

[14] Behrouz A. Forouzan Debdeep M ukhopadhyay ,cryptography and network security,2e, Mc Graw Hill Education (India) Private Limited.