A Hybrid Image Security Method Using Arnold Transform and RSA Algorithm

Bhavesh Jain, Kanak Giri
Department of Computer Science and Engineering, Swami Keshvanand Institute of Technology, Management and Gramothan, Jaipur-302017 (INDIA)
Email - bhaveshjain678@gmail.com, kanakgiri88@gmail.com
Received 31.01.2019 received in revised form 28.02.2019, accepted 03.03.2019

Abstract: Today, people all over the world want to exchange information, but they are concern about security aspects while sharing the information or an image. In this paper, present a hybrid technique of image encryption using the Arnold Transformation and RSA Algorithm. In this proposed method first, scramble the digital image using Arnold's transformation after that encrypted that digital image using an asymmetric RSA algorithm. The proposed method is safer and the result of the resulting encrypted image is improve and safer as shown in this Paper.

Keywords: Cryptography, Decryption, Encryption, Image Encryption, RSA, Arnold Transformation

1. INTRODUCTION

In any case, the world is digitized. Each division of government agencies and private companies search for digital images using each department as a method to transfer all important data. These online images are not secure. Therefore, it is necessary to protect the image. With the rapid growth of digital communication and multimedia applications, security becomes an important issue in the transmission and storage of images. Cryptography is a way to give high security. Images are use in many areas, such as medicine and military science. The latest encryption technology provides technology to protect information and multimedia data. In recent years, cryptography technology has evolved rapidly and many image encryption methods are use to protect sensitive image data from unauthorized access.

Images are the most widely used for information sharing in various fields, such as medical, research, industrial and military fields. Various images are transfer using unsecured Internet. So, therefore it is necessary to set up proper security approach that can prevent unauthorized persons from accessing important information. So therefore advantage of the proposed approach is that it secures and protects more multimedia information. Encryption is a form of image security that provides a secure way to send and save images online. Security is the main concern of the system to support image integrity, confidentiality and originality. Encryption is the most effective way, but security issues will also appear if more gray-level data is use [1-4].

2. ARNOLD TRANSFORMATION

We can define Arnold transformation as follows. Let (x, y) is pointing in the unit square. It move to the (x', y') by the following equation [5].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Where N is the length of the square unit. This conversion called is Arnold's 2D conversion. For digital images, the Arnold transformation can be defined as follows. Using the next transformation [1 1], move the pixels of the square digital image I = [I i, j]NXN to (i, j).

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Arnold's conversion is a periodic mapping and reverse. In addition, the Arnold conversion is valid for square images only. Arnold's conversion is used to encode digital images, especially for digital watermarks. Many articles believe that Arnold's conversion period is <N2. However, the article provides a linear approximation of the Arnold period corresponding to equation 3, as in [5].

$$T = 1.4938N + 40.8689$$
$$2 \leq N \leq 2000 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

According to Arnold's concept of conversion, the encode of the place space corresponds primarily to the first place of the pixels of the transferred image. The degree of overlap is greater if the pixel moves outside the pixels of the original image. Encoding does not change the gray level of the pixels in the original image, but you can change the visual effect image. Image encoding compares the original image to "chaos" and indicates that the random algorithm is more efficient. As a result, the scrambling function makes the pixel image a disaster. As a result, Arnold's conversion is use to

increase image protection. The basic flow chart for the hybrid image appears with Arnold turning in the fig. 1.

Arnold's conversion is primarily used to encrypt images to protect images using image encryption techniques. The results obtained and the Arnold conversion simulation is shown in the fig. 2.

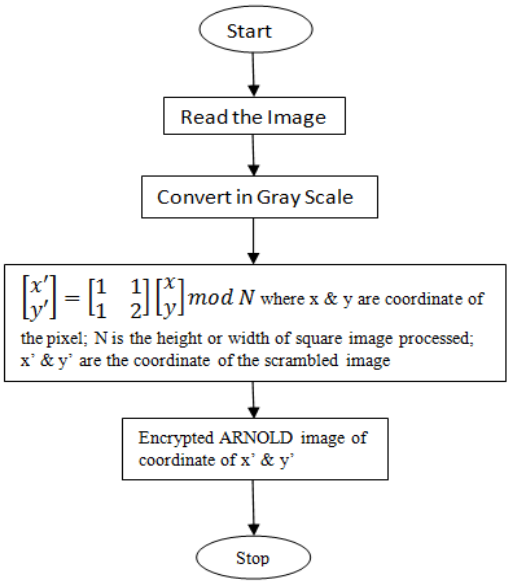

Figure 1: Flow Chart of Image scrambling Using the Arnold Transformation

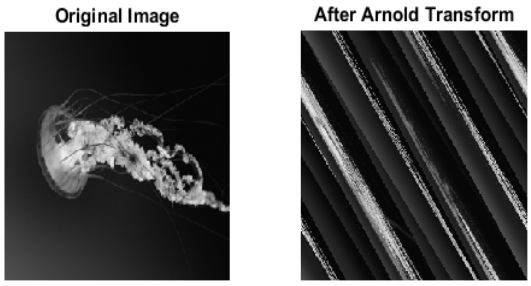

Figure 2 : Original Image and image scrambling after Arnold Transformation

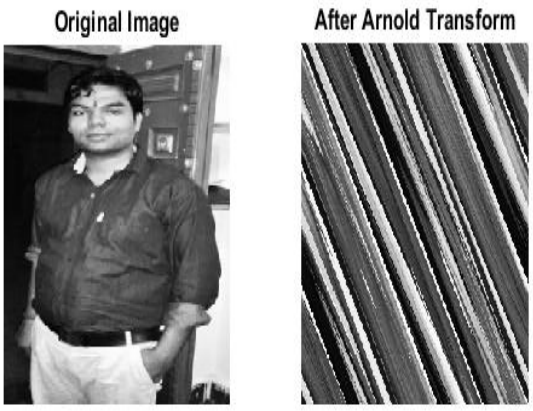

Figure 3 : Original Image of person and scrambling image of person after Arnold Transformation

3. RSA ALGORITHM

Public-key cryptography is also called asymmetric. To do this, you need to use a secret key (a key known only to the owner) and a public key (a key known to all). Public-key cryptography is a basic technology widely used all over the world. This method is use in many cryptographic algorithms and is widely used in software security, financial transactions and other important security areas where it is important to protect against forgery and falsification.

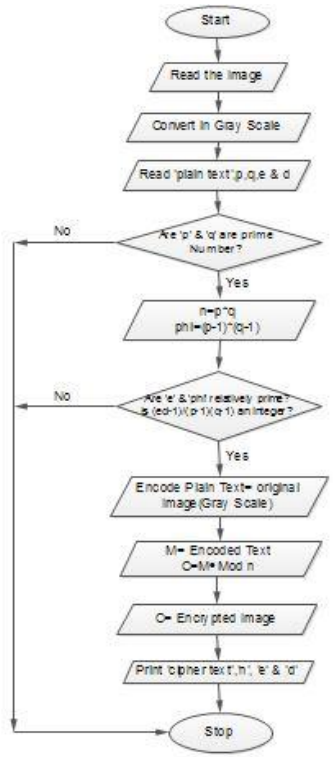

Figure 4 : Flow Chart of RSA Algorithm

RSA is the first known cryptography and encryption algorithm, one of the first major advances in public-key cryptography. We use a pair of keys, one used to encrypt the image and can only be decrypted using the other keys of the pair [7].

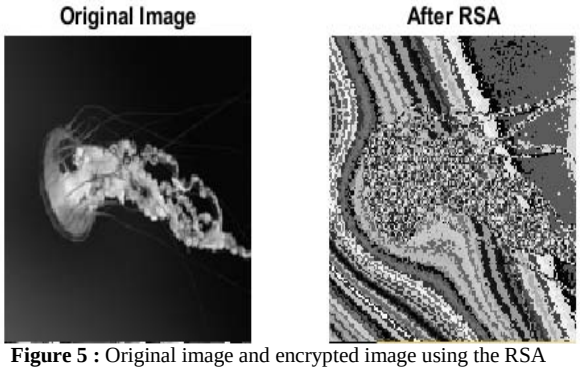

Figure 5 : Original image and encrypted image using the RSA Algorithm

RSA is one of the most commonly used algorithms for digital image security or digital image encryption. Encryption is one of the best ways to protect data and images while you're connected. In an encrypted image, no one can see the original data or image there. To see the original data or images, you can use the decryption technology to get the original image from the encrypted image.

The Basic Flow chart of image encryption using the RSA Algorithm is shown in fig. 4.

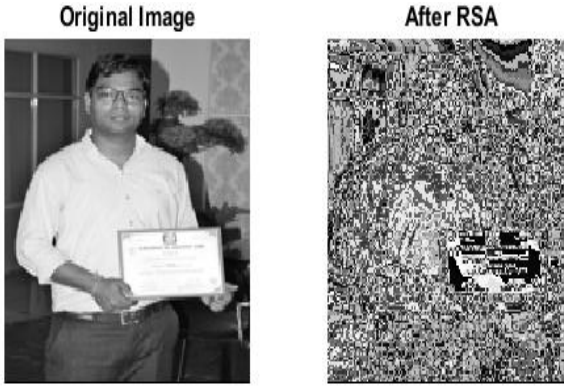

Figure 6: original image and encrypted image of a person using the RSA Algorithm

4. PROPOSED IMAGE ENCRYPTION TECHNIQUE

The asymmetric RSA encryption algorithm makes encryption more secure, and recipients are less afraid of giving each sender a different connection key. Another advantage of the RSA algorithm is that it is difficult to decrypt because the RSA algorithm includes a key reason that is difficult to reproduce. Using permutations or hacking attempts by one or the other, can get a decryption key, which is almost the same as the original key. It can exit and decode 70-80%. Then, there is the possibility that you can understand the real picture (or you can say the image has been decrypt) [8-9].

So, to solve this problem, we will use another Arnold conversion technique here. According to Arnold's concept of conversion, the encode of the place space corresponds primarily to the first place of the pixels of the transferred image. The degree of overlap is greater if the pixel moves outside the pixels of the original image. Encoding does not change the gray level of the pixels in the original image, but you can change the visual effect image. Image encoding compares the original image to "chaos" and indicates that the random algorithm is more efficient. As a result, the scrambling function makes the pixel image a disaster. That's why hackers can understand real images (70 to 80% before Arnold's reverse shift). It is very difficult to understand the image of the problem and penetration. Another advantage of converting Arnold is the normative use. Therefore, if the pirates should know how often Arnold's distortion is repeat. If you're planning the wrong number at a later time, try making the image more complex and confusing.

The Flow Chart of the proposed design methodology is shown in fig. 7.

Therefore, the proposed method uses Arnold transform and asymmetric RSA algorithm. The results obtained from the proposed image encryption method are shown in fig. 8.

5. CONCLUSION

In this Paper we showed the various analyses of image encryption results using Arnold transformation algorithm and asymmetric RSA algorithm.

The asymmetric RSA encryption algorithm makes encryption more secure, and recipients are less afraid of giving each sender a different public key. Another advantage of the RSA algorithm is that it is difficult to decrypt because the RSA algorithm includes a key factors that is difficult to reproduce. Using permutations or hacking attempts by one or the other, which can get a decryption key, which is almost the same as the original key. It can exit and decode 70-80%. Then, there is the possibility that you can understand the real picture (or you can say the image has been decrypt).

So, to solve this problem, we will use another Arnold conversion technique here. According to Arnold's concept of conversion, the encode of the place space corresponds primarily to the first place of the pixels of the transferred image. The degree of overlap is greater if the pixel moves outside the pixels of the original image. Encoding does not change the gray level of the pixels in the original image, but you can change the visual effect image. Image encoding compares the original image to "chaos" and indicates that the random algorithm is more efficient. As a result, the scrambling function makes the pixel image a disaster. That's why hackers can understand real images (70 to 80% before Arnold's reverse shift). It is very difficult to understand the image of the problem and penetration. Another advantage of converting Arnold is the normative use. Therefore, if the pirates should know how often Arnold's distortion is repeat. If you're planning the wrong number at a later time, try making the image more complex and confusing.

Therefore, the proposed method uses Arnold transform hybrid and asymmetric RSA algorithm. The results obtained by the proposed image encryption method are safer and improved.

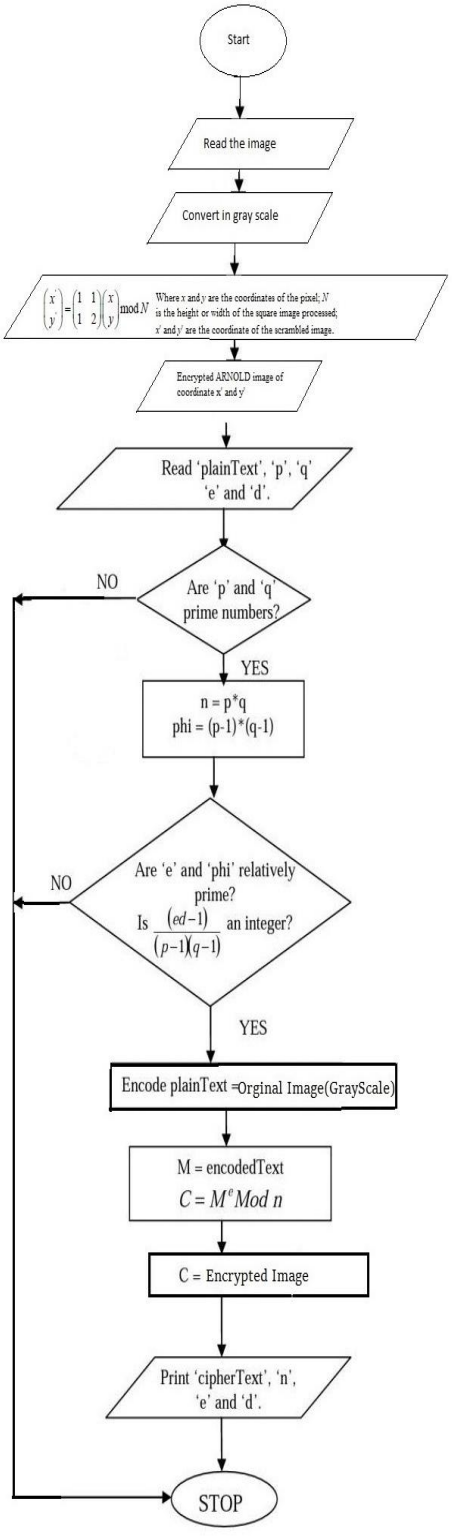

Figure 7: Flow Chart of proposed design methodology

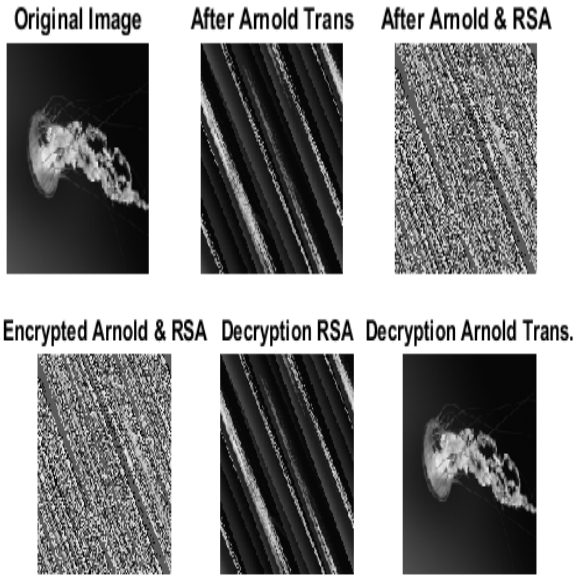

Figure 8 : Encryption and Decryption of Image using Arnold Transformation and RSA Algorithm

REFERENCES

[1] Prabhat K. Panda, "A Hybrid Security Algorithm for RSA Cryptosystem", IEEE International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Coimbatore, INDIA, (2017), 1-6.

[2] Vishal Goar, Manoj Kuri, Shikha Mathur and Deepika Gupta, "Analysis And Design Of Enhanced Rsa Algorithm To Improve The Security", 3rd IEEE International Conference on Computational Intelligence and Communication Technology,(2017),1-5.

[3] Souvik Sinha, Shankha Mukherjee, Shakya Chakrabarti and Tamal Mukhopadhyay, "A meticulous implementation of RSA Algorithm using MATLAB for Image Encryption", IEEE, (2017), 1-6.

[4] Srikanta Murthy K., Ganga Holi and Madhu B., "An Overview of Image Security Techniques", International Journal of Computer Applications, (2016), 154(6), 37-46.

[5] Sangita A. Jaju and Santosh S. Chowhan, "A Modified RSA Algorithm to Enhance Security forvDigital Signature", IEEE, (2015), 1-5.

[6] Bhanu Kapoor and Sapna Saxena, "An Efficient Parallel Algorithm for Secured Data Communications Using RSA Public Key Cryptography Method", IEEE International Advance Computing Conference, (2014), 850-854.

[7] Rohit Minni, Saurabh Mishra, Kaushal Sultania and Durai Raj Vincent PM, "An Algorithm to Enhance Security in RSA", IEEE 4th ICCCNT 2013, VIT University,(2013), 1-4.

[8] Khalid Hamdnaalla1, Abubaker Wahaballal and Osman Wahballa1, "Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithm", International Journal of Video & Image Processing and Network Security, (2013), 13(4), 6-17.

[9] Yongping Qiu, Yunfeng Xue and Qiudong Sun, Ping Guan, "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling", IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery, (2012), 1669-1672.