International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-4, Issue-4, April 2018 Pages 86-90

# Image Encryption based on Chaotic Systems and Shuffling Algorithm

**Anish Batra, Siddharth Gorey, Ms. Reena Singh**

*Abstract*— **The process of encoding any given piece of information or data using a particular selection of available algorithms is known as encryption. The motive is to ensure that the message only reaches the actual receiving audience for which it was intended in the first place and even if the transmission pathway is compromised in one way or another and an unauthorized party is somehow able to get hold of the data,it should be nothing more than gibberish for them. Our research paper focuses on image encryption in particular. With the huge plethora of images being shared today with many containing sensitive and confidential information, the need of image encryption has never been higher. Further, with computational power increasing exponentially with every year passing, older encryption schemes may not always offer the security and protection that they once did. Hence constant up gradation and improvement of encryption algorithms is the key to ensuring security. Further, encryption algorithms that work for textual data aren't as efficient or effective when used for encrypting images. Extensive previous research has been done on image encryption algorithms, we intend to build upon that research. Initially the researchers were focused on chaotic systems for image encryption using either Lorenz or Rossler chaotic systems. As time progressed, several combinations of Lorenz and Rossler started emerging. Separate algorithms were also developed that focused on shuffling algorithms with and without s-boxes. In our paper, we will utilize a combination of Lorenz and Rossler, couple it with shuffling algorithm and apply s-box shuffling over and above these to encrypt a gray scale image. This effectively gives us a three layer encryption thereby providing hugely improved security.**

*Index Terms*— **Lorenz, Rossler, Chaotic systems, s-box, Shuffling algorithm.**

## I. INTRODUCTION

With the advent of high speed Internet connection and hand held smart phone devices being within the reach of almost every single individual, the number of images being shared on a daily basis has practically exploded from a few hundred images few decades ago to more than a billion images being shared on whatsapp messenger alone. More often than not, these include private, sensitive or confidential information which if accidentally fallen into the wrong hands, could lead to disastrous consequences. This is where the widespread need and necessity of image encryption arises. Also, the previously used algorithms for test encryption may not be very successful for image encryption simply because of the fact that the images have special storage characteristics and weakness of low level efficiency, especially when image is large. Hence the chaos based approach was suggested to enable highly secure fast and efficient image encryption. Chaotic systems are usually designed to work on either Lorenz chaotic systems or Rossler chaotic system or a combination of those. In our paper, we will be using a combination or Lorenz and Rossler which will be discussed in the upcoming sections. Further, to make the encryption even more secure we will also be applying shuffling algorithm with s-boxes. This makes the encryption a three tier process thereby greatly improving security.

especially when image is large. Hence the chaos based approach was suggested to enable highly secure fast and efficient image encryption. Chaotic systems are usually designed to work on either Lorenz chaotic systems or Rossler chaotic system or a combination of those. Further, research has also been done on shuffle algorithms along with s-boxes for image encryption all of which we will be using here and building upon them.

**Our Contribution.** 1) We will be working out a combination of Lorenz and Rossler chaotic systems in which each of them will have a different multiplication factor. 2) After applying the chaotic approach on the image to be encrypted we will be applying shuffle algorithm. 3) After that is done, we will applying s-box shuffle on the resultant, thereby making it a three tier encryption process.

**Organization.** Section II discusses the problems with current image encryption algorithms; section III discusses the corresponding solution, whereas section IV describes in detail the technical implementation; section V discusses future scope, and concluding remarks are found in section VI.

## II. THE PROBLEM WITH CURRENT IMAGE ENCRYPTION ALGORITHMS.

**Related Work.** Extensive work has been done previously on the subject of image encryption. Earlier attempts focused on applying the previously used algorithm like DES to encrypt images as well. However it was soon found to be ineffective because of the fact that the images have special storage characteristics and weakness of low level efficiency, Viewed in isolation, most current image encryption algorithms work perfectly well. The problem emerges as we move forward in time. Computers are becoming exponentially powerful day in and day out. What this means is that even though the encryption algorithms of today make it impossible for present day computers to breach them, there will come a time in future when they would no longer be adequate. And that time is going to come sooner than we think. Hence encryption algorithms need to continuously evolve in complexity and resilience so as to withstand the enormous computing power of future computers. That is exactly what our paper focuses

**Anish Batra**, Bharati Vidyapeeth's College of Engineering, New Delhi, India
**Siddharth Gorey**, Bharati Vidyapeeth's College of Engineering, New Delhi, India
**Ms. Reena Singh**, Bharati Vidyapeeth's College of Engineering, New Delhi, India

on. By combining three existing image encryption approaches into one, we will not only be able to increase complexity but will also in turn improve security.

## III. SOLUTION: THREE TIER COMBINATION

We will be working on a combination of available approaches for image encryption. Firstly we will be employing the chaotic system using a combination of Lorenz and Rossler chaotic systems. After that we will be applying the shuffle algorithm to the resultant followed by the application of s-box to obtain the final encrypted image. This three tier encryption will make the encryption significantly more secure.

## IV. IMPLEMENTATION

The original grayscale image that we started the encryption process with:

Fig 1. Sample image 1

We first began by developing a combination of Lorenz and Rossler chaotic systems. Before we proceed to that, we need to see the Lorenz and Rossler equations.

The Lorenz equations are as follows:

$$\dot{x}=(sigma)(y-x) \quad (1)$$

$$\dot{y}=rx-y-xz \quad (2)$$

$$z=xy-(beta)z \quad (3)$$

The parameters sigma, r and beta are positive numbers and are chosen arbitrarily. For this exercise we have chosen them as follows:

$$sigma=10 \quad (4)$$

$$r=28 \quad (5)$$

$$beta=8/3 \quad (6)$$

This system of differential equations will then be solved using runge kutta method in gnu octave.

The Rossler equations are as follows

$$x=-y-z \quad (7)$$

$$y=x+ay \quad (8)$$

$$z=b+z(x-c) \quad (9)$$

The values of a, b, c are as follows:

$$a=b=0.2$$

$$c=5.7$$

We will now propose a combination of these two equations such that a more complex set of chaotic systems could be obtained by their combination.

The proposed combination will be of the form:

VARIABLE = 2*(Lorenz chaotic system) + (Rossler chaotic systems)

Which effectively gives us the following combined equations:

$$x=2*(sigma)(y-x)+(-y-z) \quad (10)$$

$$y=2*(rx-y-xz)+(x+ay) \quad (11)$$

$$z=2*(xy-(beta)z)+(b+z(x-c)) \quad (12)$$

It is a universal belief that chaos is the period independent long term behavior that shows dependence on some initial conditions. These are the arbitrary parameters in the above equation.

Further, the security of Each Lorenz and Rossler individually depends on three arbitrary parameters when utilised in isolation. Whereas, in the above scenario where they have been combined, the resultant equations is dependent on 6 parameters thereby massively boosting the efficacy of chaotic systems. Hence this is already more secure method of image encryption than either Lorenz or Rossler chaotic systems when viewed in isolation.

The objective of the upcoming step is to encrypt the output image subjected to chaotic systems by the shuffling algorithm and then changing the gray scale values to create the second tier encrypted image. Before applying the actual shuffling algorithm we add another step in the process in order to further boost the security of the encrypted image which can be described as follows: We XOR the chaotic mask and the original image thus further adding an additional step and improving the complexity of decryption. The following image shows the implementation of the s-box.

Now we will proceed to applying the shuffling algorithm on the given image. A Rijndael s-box is a lookup table which transforms one set of given values in the range of 1 to 256 to another set of values in the same range. It acts as an invertible

map of values so that later on we can lookup the inverted values again from the s-box.

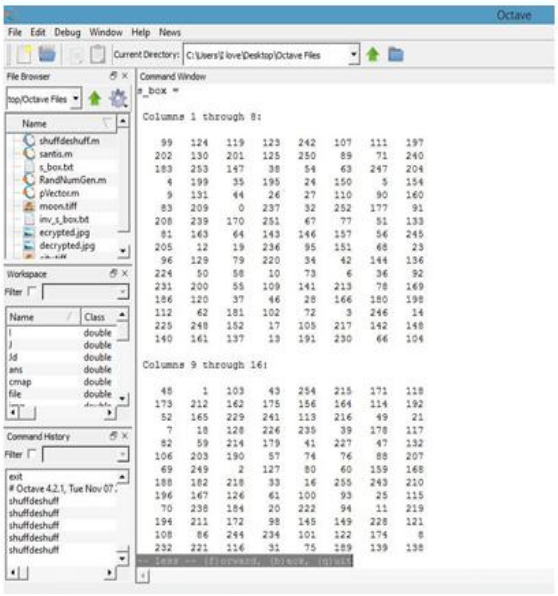

Fig 2. S-box representation.

After sorting the image pixels and re-transforming it to a matrix, we store a set of keys which represents the offsets for the individual pixels. Now, we look up each value one by one in the matrix of the image and we find the lookup value from the s-box table. For each intensity value, we find the left nibble and the right nibbles, the left nibble acts as the row lookup and the right nibble acts as the column lookup. The lookup value replaces the individual values of intensity in the matrix of the image. This process is repeated for each key value given as an input by the user.

After the successful application of each of the steps above we obtained the following encrypted image which is completely illegible.

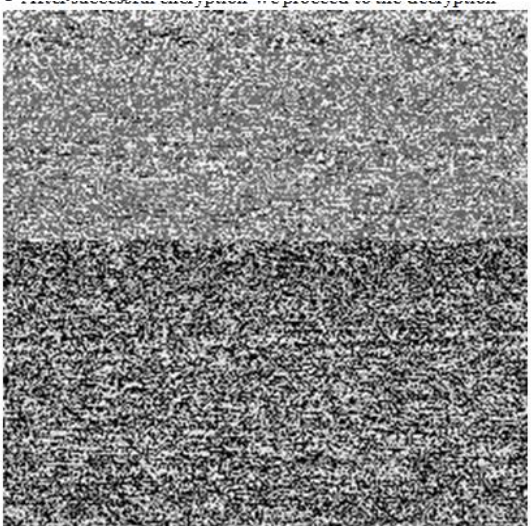

Fig 3. Encrypted image for Fig 1.

After successful encryption we proceed to the decryption process. For the decryption process we perform the inverse function of the steps we performed while undertaking the process of encryption in the exact reverse order. That is we begin with the inverse s-box process which is the reverse of s-box designed to map the values replaced by the s-box in the encryption process to their respective corresponding original values.

Once the effect of s-box is removed we proceed to undoing the effects of shuffle algorithm followed by taking the exact no. of XOR iterations as taken previously during the original process. After this we arrive at our last step of decryption that is undoing the effect of application of chaotic system on the sample image. This imvolves subjecting the illumination values of every pixel to the inverse function of the combination of Lorenz and Rossler function that we subjected our sample image to during the encryption phase. Once the decryption process is completed successfully we will arrive at the original sample image.

The following is a snapshot of the code we executed on gnu octave in order to implement the project:

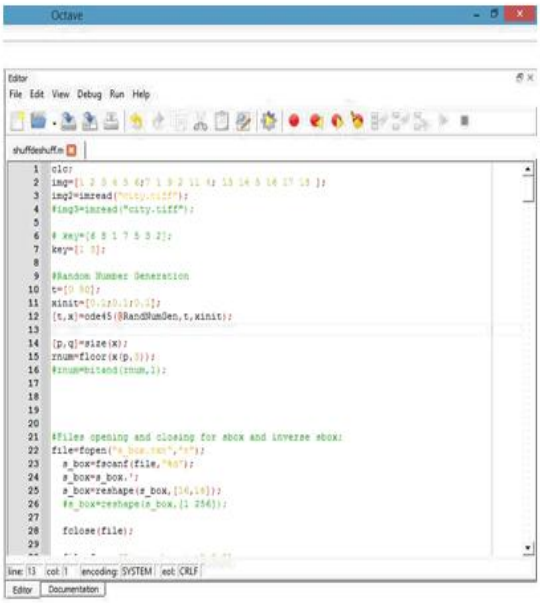

Fig 4. Implementation of the algorithm

This is the image obtained after the decryption process was complete:

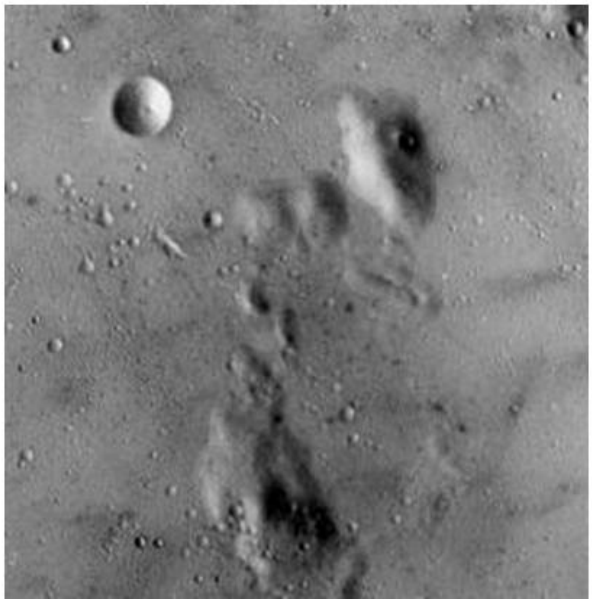

Fig 5. Decrypted image for Fig 1.

## V. FUTURE SCOPE

As discussed before, image encryption is going to play an ever increasing and larger role in modern society. Its necessity has been proved without the slightest sliver of doubt. The algorithms of today may offer good enough protection against the present day computers but they might not stand a chance against future computing power. Hence increased complexity of image encryption algorithms holds immense and far reaching future scope. Further, it needs to be realised and understood that the complexity of algorithms has to be progressively increased as we move forward. Hence this is a continuous process and not a one time solution. So the future projects will build upon the researches of today and further improve the security. Hence the future scope is correspondingly massive.

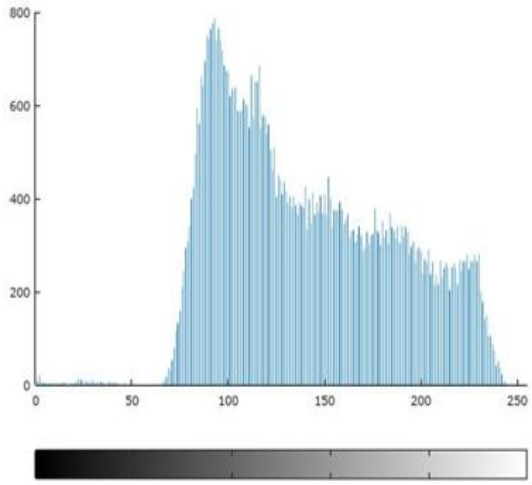


Fig 6. Histogram of the original image.

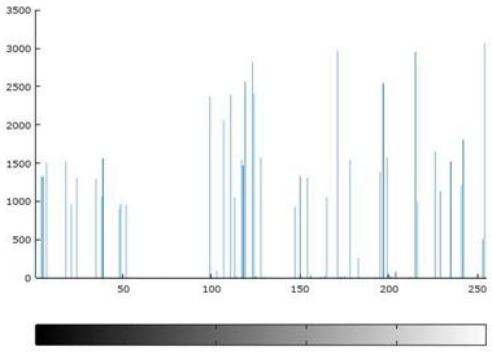


Fig 7. Histogram of the encrypted image.

## VI. HISTOGRAM ANALYSIS

The histogram analysis is shown in the following figures.

## VII. COVARIANCE ANALYSIS

The covariance analysis has been shown in the following figures.

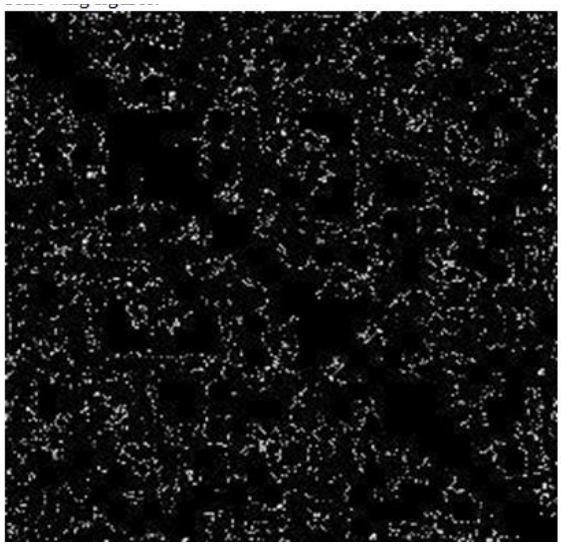

Fig 8. Covariance of the original image.

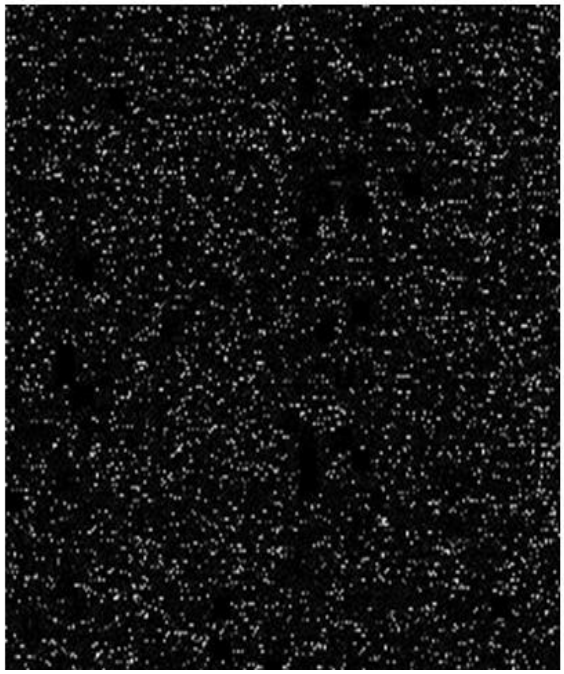

Fig 9. Covariance of the encrypted image.

## VIII. CONCLUSION

We began byexplaining the need for more complex algorithms for image encryption and then went onto demonstrate the work that has been done already. These included the chaotic system approach involving Lorenz or Rossler systems, shuffle algorithms and s-box substitution. We then went on to present and and implement an algorithm that successively uses all three of these approaches and applies them onto the image one after the other thereby giving us a new algorithm designed by their combination which is many times more complex and resistant to attacks by both present and future computers thereby boosting security.

## REFERENCES

[1] Qais H. Alsafasfeh and Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems" Journal of Signal and Information Processing, 2011, 2, 238-244. doi:10.4236/jsip.2011.23033.

[2] Abdelfatah A. Yahya and Ayman M. Abdalla, "A Shuffle Image-Encryption Algorithm" Journal of Computer Science 4 (12): 999-1002, 2008 ISSN 1549-3636.

[3] Chen, G., 2008. A novel heuristic method for obtaining S-boxes. Chaos Solit. Fract, 36: 1028-1036. DOI: 10.1016/j.chaos.2006.08.003.

[4] Federal Information Processing Standards (FIPS 197), 2001.The Advanced Encryption Standard. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf 6.