[1] Apoorv Kumar *
[2] Dr. Adarsh Patel
[3] Dr. Shahana Gajal Qureshi
[4] Dr. D. Saravana

Analysis of the Impact of Logistic Map with Gaussian Membership Function for Cryptography

Journal of Electrical Systems

Abstract: - This paper deals with the integration of the as logistic map with the different fuzzy number generators, resulting in a hybrid approach of encryption that can leverage the strengths and randomness of both chaotic dynamics and fuzzy logic. The chaotic maps are influenced by the Gaussian fuzzification, which produces bifurcation diagrams that have the fundamental structure of the system's dynamics. By analyzing the chaotic behavior of the various maps and their impact on generating the pseudo-random sequences which can be suitable for the encryption, the fuzzy numbers are added to modify the chaotic systems. The proposed hybrid encryption approach is expected to address the limitations of single chaotic map usage and thus to represent a more effective and efficient encryption approach. The proper security analysis and cryptanalysis of the chaotic encryption algorithms are very important to recognize probable vulnerabilities at the very beginning. Optimization methods for a particular device i.e., GPUs (Graphics Processing Units) or FPGAs, as well as parallel processing exploration, will be the key to improving these algorithms in real-world applications.

Keywords: Gaussian fuzzy number generator, Gaussian Membership function, Logistic map, nonlinear dynamic equation, Logistic and Gaussian image encryption.

I. INTRODUCTION

Rapid expansion of digital communication in multimedia transmission over the internet has led towards growing demands in robust encryptions techniques for safeguarding the sensitive information. The complexity of the cyber threats increases, traditional methods became less effective which ensures data privacy and integrity, particularly true in the realm of image encryption in which high volumes of data and real time processing requirements poses the significant challenges in existing system of cryptography. Therefore, many researchers are exploring new and more advanced methods and techniques which combine multiple approaches in strengthening the encryption mechanism and improve its resilience towards modern cryptographic attacks.

Most promising development in this cryptography field is the use of the chaos maps and chaos systems in which they are characterized by their initial condition's sensitivity and its ability for generating the complex and pseudo random sequences. Chaotic maps such as logistic map have already gained considerable interest due to their nonlinear behavior. It can be harnessed to disrupt the inherent correlations in image data. Logistic map which is a simple and effective polynomial mapping exhibiting chaotic behavior when its system parameter sets appropriately making it a one of the powerful tools for generating randomness [11]. This is crucial in encryption, as it introduces uncertainty in data encryption ultimately making it harder to break the encryption through conventional means.

Despite its potential, chaotic maps alone are not sufficient to provide a level of security to withstand some sophisticated attacks. The limitation of using a single chaos map is, it is predictable and deterministic. Its initial condition can lead to chaos, but the deterministic behavior can be exploited especially where the attacker knows the system parameter. Resulting chaotic systems can be enhanced by integrating them with other known or custom techniques which can introduce the additional layer of complexity and unpredictability.

Fuzzy logic, which is a mathematical framework designed to handle uncertainty and imprecision, has proven to be an effective tool in augmenting the chaos maps. These generators create degree of membership rather than binary true or false and can introduce element of variability into chaotic system. Applying the fuzzy number generator to the chaotic system one can achieve a hybrid system which can benefit from unpredictability of chaos and adaptability of the fuzzy membership function. This type of combination can allow for users for more secure

[1] VIT Bhopal University, School of Computing Science Engineering and Artificial Intelligence, Bhopal, India. apoorv.kumar2020@vitbhopal.ac.in
[2] VIT Bhopal University, School of Computing Science Engineering and Artificial Intelligence, Bhopal, India. adarsh.patel@vitbhopal.ac.in
[3] VIT Bhopal University, School of Computing Science Engineering and Artificial Intelligence, Bhopal, India. shahana.qureshi@vitbhopal.ac.in
[4] VIT Bhopal University, School of Computing Science Engineering and Artificial Intelligence, Bhopal, India. saravanan.d@vitbhopal.ac.in
* Corresponding Author Email: apoorv.kumar2020@vitbhopal.ac.in

encryption methods by adding fuzzy membership function as a dynamic component which can continuously modify the behavior of chaos system and making it more resilient to attacks.

This research explores the integration of fuzzy number generators, Gaussian fuzzy number generator with simple non-linear chaos system. By integrating them to each other can create hybrid controllers or ecosystems for nonlinear dynamics which can be useful in the field of cryptography [7]. The object is to combine these fuzzy membership functions such that it can help to create a secure and efficient encryption system

II. Literature Review

Logistic map is one of the most common map which is a non linear type of chaos map commonly used for generating chaotic sequences with Some modification as we can see [1,6] By applying some modification in the logistic map one can drastically changes hits chaotic properties and making it much more unpredictable and random which is essential for encryption of the image

The paper [1] modification of logistic map using fuzzy numbers with application to Pseudo random numbers generation and image encryption authors Moysis, L., Volos, C., Jafari, S., Munoz-Pacheco, J. M., Kengne, J., Rajagopal, K., & Stouboulos, I discuss regarding enhancement of the chaotic behaviors of logistic map by introducing phenomena Like crisis and randomness. The methodology they use is adding triangular fuzzy numbers through logistic map which eventually enhances the chaotic behavior of the logistic map which can lead to complex phenomena like chaos. Their study extends its application by applying it in encrypting an image from the generated bit sequences using XOR operation in a grayscale image effectively. This type of modification results in higher Lyapunov of exponent when compared to classical Logistic map The modified logistic map introduced is analyzed through its platform exponent and bifurcation diagrams which demonstrate the increase in complexity compared to the original logistic map this research may also apply in generation of pseudo random bit sequences which eventually passes NIST Statistical test successfully furthermore the authors' Study delves into image encryption using bits generated by their methodology of logistic map showcasing the security and effectiveness of the proposed approach the paper also highlights the versatility and potential application of their approach in various field emphasizing the contribution in Chaos theory and cryptography.

A new parallel fuzzy multi modular Chaotic Logistic map for image encryption [2] authored by Gad, M., Hagras, E., Soliman, H., & Hikal, N Introduced a novel image encryption algorithm called parallel fuzzy multinodular chaotic logistic map in this type of algorithm they combine chaotic system and fuzzy logic to enhance its security in image encryption and its applications. The author designs a new chaotic system based on hybrid CCS and DPCCS technique. The encryption process of this paper involves diffusion confusion mechanism with controllable iterative parameters for the are Arnold cat map. The proposed methodology demonstrates robust chaotic properties with complex bifurcation diagram and high Lyapunov exponent which ensures high level of security and complexity in image encryption. They are proposed scheme has evaluated through statistical test, random analysis and key sensitive analysis to ensure security and performance. The methodology offers a large key space which is effective against statistical attacks and high sensitivity to key change make it suitable for secure image encryption.

Control of chaos: Methods and applications in engineering [3] authors Fradkov, A.L.; Evans, R.J. Performs a comprehensive overview of the fear of chaos control detailing its historical development, key methodologies and various applications across different engineering disciplines. The author outlines the current state of research in chaos control highlighting significant challenges and encourage for further exploration in the Chaos regime. The paper categories chaos control methods in several key approaches such as feedforward control, OGY method, Paragas method Nonlinear and adaptive control. The author also emphasizes the wide range of applications of chaos control across various fields including chemical engineering, mechanical engineering electrical engineering, telecommunication and information systems. The author also discusses challenges and future direction in chaos studies, and he also noted that there are many challenges remaining in this field. The author also noted that most of the studies in this field are computer simulated rather than rigorous analytical proofs leading a lack of comprehensive understanding of the underlying principles they also highlighted the need for further research to address the unresolved problems.

Discrete fractional logistic map and its chaos[4] authored by Wu, G.C.; Baleanu, D Studies and investigates the dynamics of fractional delay logistic maps and focusing on the emergence of its chaotic behavior the author also utilizes discrete fractional calculus to formulate a fractional difference equation which can extend the classical logistic map by incorporating memory effects through delayed parameter. They concluded that the discrete fractional calculus which provide a powerful tool for modelling complex dynamical system with memory effects highlighting the rich dynamics that can arise from incorporating fraction orders and delayed into traditional models.

The authors also suggested that this insight might have implications for understanding real world phenomena in field of ecology where population dynamics often exhibit complex behavior.

An image encryption algorithm based on modified logistic chaoti1c map [5] author Han, C. Presents a novel image encryption algorithm that uses modified logistic map to enhance security of image and encryption first stop the author also addresses its key limitations of traditional encryption methods particularly the issues of small key space and vulnerability to statistical analysis first stop the author employees scrambling and diffusion model which leverage the chaotic sequence to generate scrambled key matrices essential for encryption processes. The proposed methodology validates the effectiveness of algorithm by revealing that it offers infinite key space and demonstrates high key sensitivity which makes it more resilient against exhaustive attack.

III. Methodology

Logistic map, which is a polynomial mapping of 2nd degree also often referred to as an archetypal example of complex, chaotic behavior can arise from very simple non-linear dynamical equations. It was introduced firstly by Pierre François Verhulst in the 19th century describing the population growth in a confined environment. The model gains its attention in the 1970s when Robert May, a biologist who studies its chaotic behavior leads to understands deeply of simple deterministic systems which can lead to complex and unpredictable results.

$$x_{n+1} = rx_n(1 - x_n)$$

x_n representing the value at iteration n and also, the ratio of an actual population to theoretical maximum population that is carrying capacity.

r which is a parameter called growth rate and typically the values should range from $0 \leq x_0 \leq 4$

For virtualizing the logistic map, computing power should be sufficient such that it can fully virtualize it, containing finite computing precision and use for adopted digital arithmetic [10].

This equation captures two effects firstly reproduction in which the increment of rate of population is proportional to the current population when the size is small and secondly starvation or density dependent mortality in which the growth rate r will decrease at rate proportional to the value obtained, taking the theoretical "carrying capacity" of the environment less the current population.

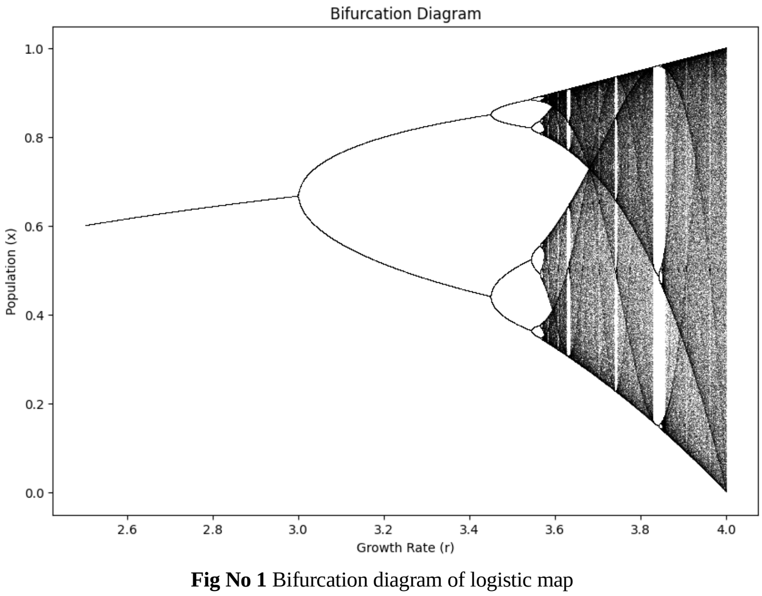

Fig No 1 Bifurcation diagram of logistic map

The behavior of the logistic map changes depending upon the growth factor r due to this the transition from order to chaos can be understood by varying its value and this behavior can be seen in the above image. The diagram starts with a single point where the value of r which splits into two, four and eventually cascades into a chaotic band. From the above diagram of the logistic map, it can be divided into six phases: -

Extinction phase: -

The range of the phase is $0 < r < 1$, during this phase the growth rate is so low that it cannot sustain a population. Regardless of the initial value of the x_o, the population dies out and it will converge to zero.

Equilibrium Point: -

In this phase ranges from $1 < r < 3$the population reaches a stable equilibrium. As the value of $r$increase the population will converge to a single point which will represent a stable population size. It will happen regardless of the initial population as long a x_o is between 0 and 1. This is represented by a single branch across the range, which indicates that the population settles into a stable and predictable value.

Period Doubling Bifurcation: -

In this phase which has range $3 < r < 3.45$system undergoes its first bifurcation. Instead of converging, the population begins to oscillate between two values which are distinct from each other. As the growth rate increases oscillation doubles which results in alteration of population between four values then eight and so on. This whole process is called period doubling which is a key route for the chaos. Each bifurcation in the system bifurcation diagram shows that the system became more complex, and it is transitioning toward becoming into chaos.

Onset of chaos

As the growth rate $r$increases in this phase, which range$3.57 < r < 4$ the system goes undergoes through more period doubling it will continue until it reaches a point where it will no longer settle into a periodic state but instead became chaotic. When the growth rate approximately reaches to 3.57 the population becomes highly unpredictable and even a small change in the value of the initial value can lead to completely different outcomes. In the bifurcation diagram it is shown as a dense, tangled pattern points which shows that there are many possible values for the population without any clear pattern in it.

Chaos with windows of periodicity

In this phase which range $3.57 < r < 4$the system became predominantly chaotic but has islands of order in which the logistic map became temporarily predictable and are called periodic windows. In the bifurcation diagram around the value of growth rate reaches 3.83 the system sets into a periodic pattern after regaining its unpredictability

Full Chaotic behavior

This phase starts when $r = 4$ whole system becomes completely chaotic. The population values are almost entire range from 0 to 1 and they are susceptible to initial conditions display a classic phenomenon called butterfly effect.

The Lyapunov exponent which measures the rate of separation of infinitesimally close trajectories in a dynamic system. Positive value for the Lyapunov exponent indicates random population changes. Small differences in initial values of population can lead to diverging outcomes, making the prediction of the values very challenging. The sharp change in the value of the Lyapunov exponent is corresponding to the bifurcation diagram of the system in the behavior of the system changes from one to another type of periodic cycle. The Lyapunov exponent graph also shows the dips in certain region which is also corresponds to the bifurcation diagram showing the periodic window or islands of stability.

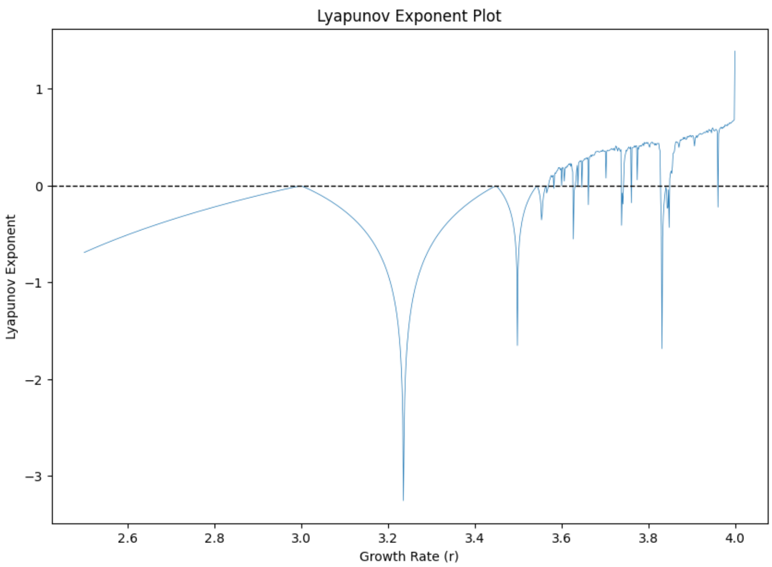

Fig No 2: Lyapunov Exponent graph of logistic map

Cobweb plots are used to visualize and analyze the convergence properties, onset of chaos and the nature of fixed periodic orbits or fixed point of the system. For the growth value $r$is 3.5 showing period doubling behavior which means that instead of converging to a single value, the iterating value starts to settle into an oscillation between multiple values. This can be shown in the cobweb plot which is represented as a red path which repeatedly forms a closed loop indicating the population values are oscillating between a set of values, but in this case, it is more complex indicating a higher periodic behavior.

If the system is tending to be converging to a single fixed point, the plot would eventually spiral and settles at a specific point on the identity line which is represented as a diagonal line, this plot shows is not showing convergences but showing a form of repetitive pattern of intersecting line. This oscillation implies that the system at 3.5 is not stable in a traditional fixed-point sense but it is stabilizing in a cycle of certain values as it can be seen at Fig no 3

As the growth rate $r$increases the behavior becomes more complex which leads to chaos as we can see from the next cobweb plot. When the growth rate is at 4 the logistic map reaches its fully chaotic behavior, the values which were visited are unpredictable and moves across wide range of values. Due to this the system became highly sensitive towards the initial conditions, which means that a tiny change in the initial value can lead to the different trajectories significantly over time, which is the hallmark for the chaotic system. This response can be seen in the next cobweb plot. In the cobweb it shows the irregular pattern, red lines are not settling in a repeating loop instead they move in an unpredictable way filling the entire phase space.

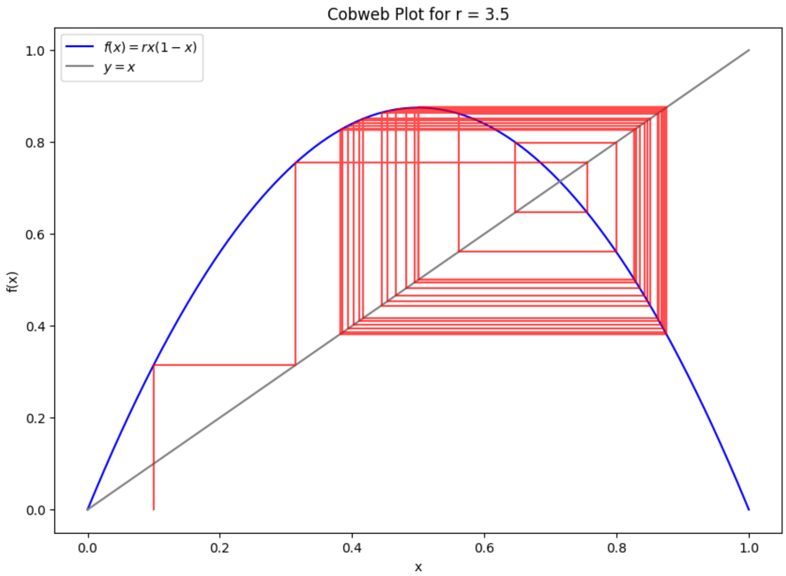

Fig no. 3: cobweb plot of Logistic map at r = 3.5

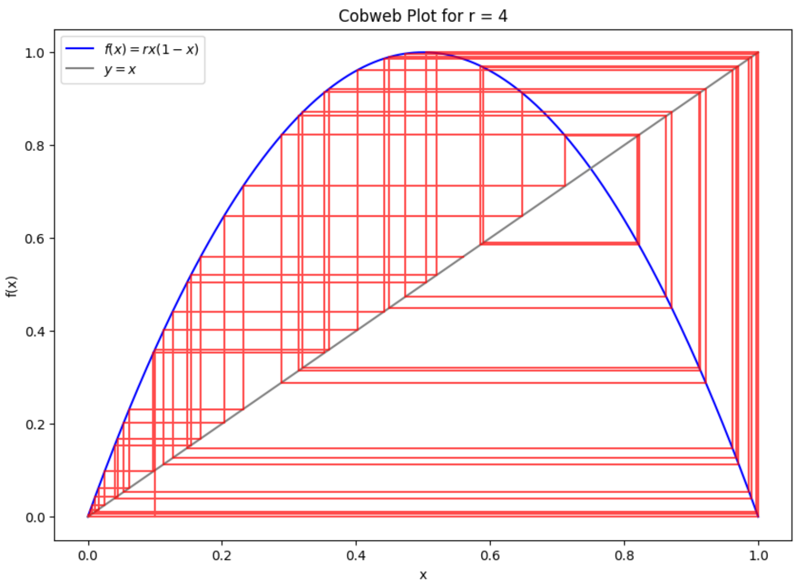

Fig No. 4: Cobweb diagram of logistic map at r = 4

The pattern of the phase space diagram is non repeated or isolated, but it is showing a dense spread of point in a continuous path which is indicating that the system will not fall into a periodic pattern when the growth rate r is set to 3.7 and the values are covering boarder range which is a hallmark for the chaotic system and due to this the system will be unpredictable for the longer term. Since points of the curve represent the outcome of a single iteration, the entire range is populating stating ergodicity in which the system will visit all the available states over the time which can been seen at Fig no 5

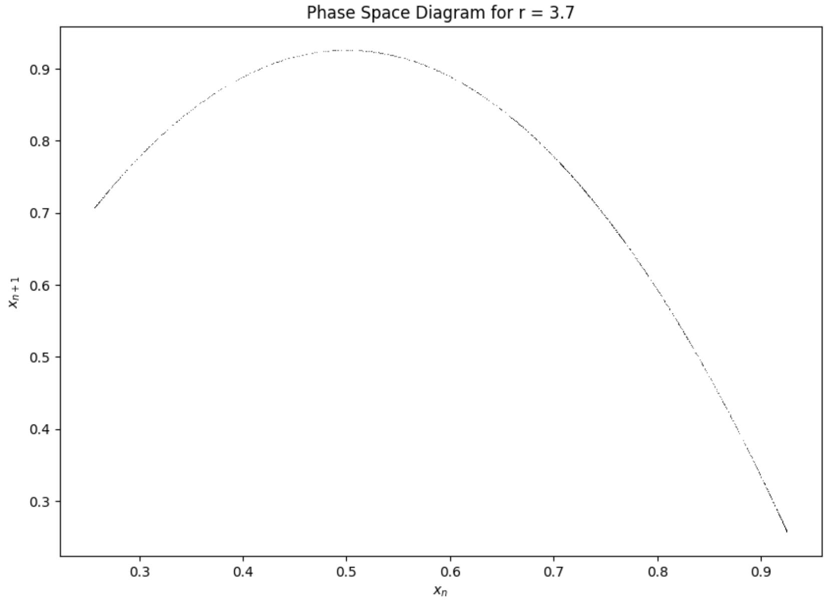

Fig No 5: Phase space diagram at r = 3.7 for logistic map

The Gaussian function which forms the basis of the Gaussian membership function introduced by German Mathematician and Physicist Carl Friedrich Gauss. A Gaussian membership function which is most used in fuzzy logic defines as the degree to which a value belongs to a fuzzy set. Characterized as smooth, bell-shaped curves, making it suitable for modeling of fuzzy set in which the gradual transition of membership's degree is needed between them. It is defined by the equation

$$\mu(x) = exp\left(-\frac{(x-c)^2}{2\sigma^2}\right)$$

$\mu(x)$ is defined as the membership function degree of the variable x in the fuzzy set
x is the crisp value or the input value
c is the curve center if the Gaussian membership function
σ σ which is defined as the standard deviation that controls the width of the curve.

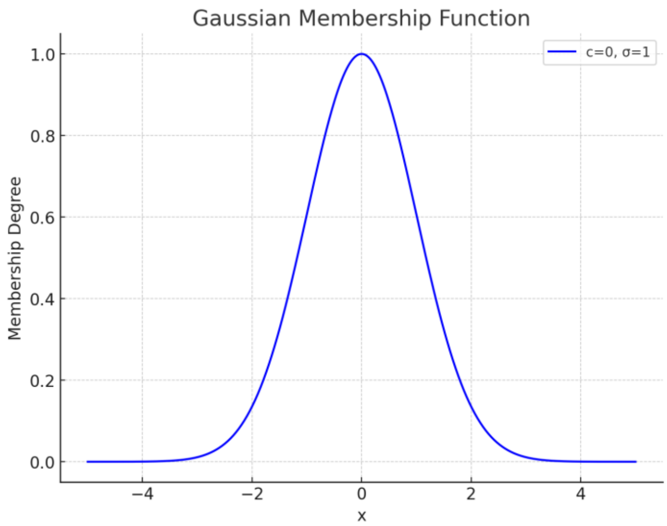

Fig No 6: Graph of the gaussian membership function

The shape of the graph is symmetric and is around the center of c when the value is 0. As it starts moving away from the center from both sides the degree of the membership function starts to decrease smoothly. This is characteristics of Gaussian membership function in which the further the input is, less it belongs to the fuzzy set. The standard deviation $\sigma$of the membership function controls the width of the curve. The smaller the value narrows the curve, which means when the membership degree moves away from the center it will rapidly decrease. One of the most important characteristics of the gaussian membership function is gradual transition between membership degrees unlike the other membership functions such as Triangulara membership function which contains sharp transitions the Gaussian has smoother decrease as one move away from the center.

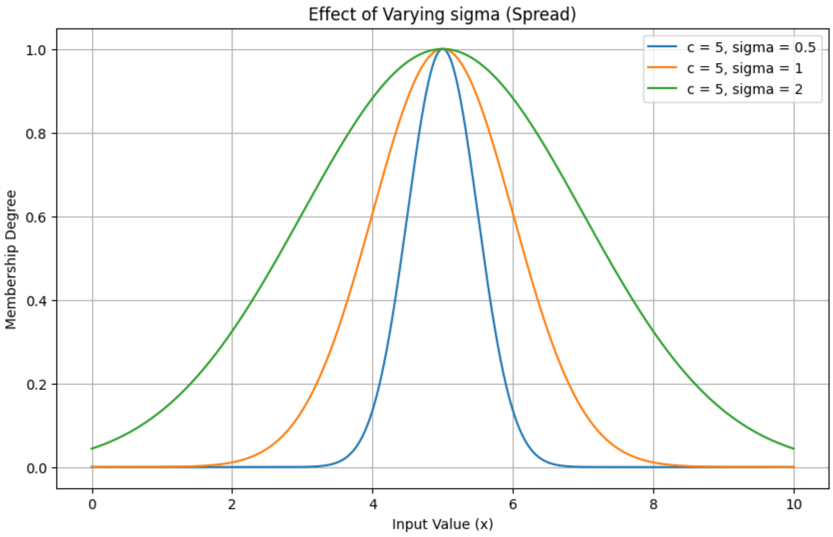

Fig no: 7. Effect of varying σ

In the analysis of the figure number a 7 is showing the center C which is constant and the effect of varying the parameter σ which is influencing the spread of the function for the value σ when it is 0.5 Which has been shown in the graph by a blue curve showed a narrow and sharply peak around the center C when it is 5. The smaller value of σ which can result in localized membership function in which a small well range of input value around C have higher membership degree that is close to 1. It explains that the function decays rapidly when the variable X moves away from the center which means the value is far away from C and have negligible membership this type of characteristic is useful in the system where the strict and precise calculation and classification is required around the center. For the σ Valley of one which is shown in the orange curve when comparing to the value of 0 .5 indicating that the membership degree has higher over the large range of input values and this type of transition from our higher membership degree from the value of 1 To allow value near zero is smoother compared to the previous case this intermediate value of σ Is offering a balance between localization and generalization of the Gaussian membership function. For the value of σ when it is 2 which has been shown in the green curve in figure 6 has the pi test curve among the other two cases with the more gradual rise to the peak and slower decline a higher value of σ result in broad membership function where a wide range of input value near the center exhibit a higher degree this type of behavior is appropriate in the cases where the broader generalization has been required and the input is further from the center which have still. The variation of the parameter in the Gaussian membership function can greatly influence the shape and the spread of the curve by adjusting the value of the σ the membership function can be tuned to meet the standard or need for a different application ranging from the precise calculation or classification to a more generalized fuzzy inference. This type of flexibility highlights the strength of Gaussian membership function in the fuzzy systems in which both accuracy and smoothness are essential for handling the uncertainty and imprecision.

The methodology we are using in combining Logistic map and the membership function is in [1] in which they are multiplying the function to the logistic map such that it is Changing the values in every iteration

$$x_{n+1} = f(z) \cdot \left(r x_n (1 - x_n)\right)$$

$f(z)$ Is representing the membership function which is mind applying to the logistic map equation.

By combining the logistic function and membership function in this case Gaussian membership one can achieve uncertainty and randomness in a Chaos system. From [1] We can combine the logistic map and the membership function such that it can influence it in every step resulting randomness and inequality in the system.

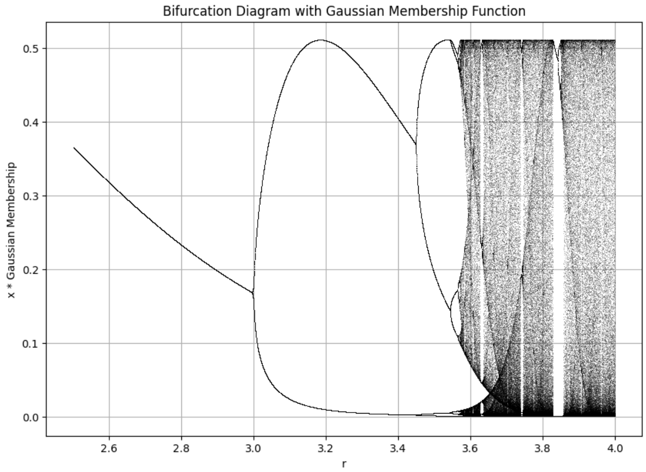

Fig no.8 Bifurcation Diagram of the logistic map influence with Gaussian membership function

The modification of the logistics map with Gaussian membership function has influenced the dynamics of the logistic map. The function is narrowing and broaden the values of the logistic map which is effectively constraining and amplifying the chaotic behavior of the map this type of transformation is Affecting the height of bifurcation branches As it can be seen in figure number 8 when the range of fuzzy membership value along the vertical axis particularly around 3.0 the membership function has a notable dampening effect the membership function also adds additional layer of complexity which is depending upon the parameter of the Gaussian that is mean and standard aviation which can either suppress or enhance the chaotic behavior or nature of the logistic map.

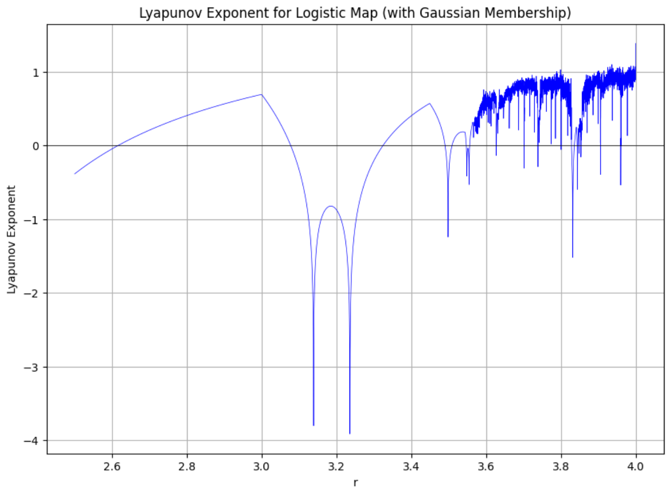

Fig No 9 Lyapunov exponent of the logistic map influenced by gaussian membership function

The chaos threshold of the lapel of exponent is marked with the red dash line at λ= 0 distinguishing the chaotic and non-chaotic regimes. When the growth rate $r = 3.2$Indicatingthat the system became sensitive to the initial conditions, but it is predictable which is the mark of the transition point where period-doubling occurs. When$r = 3.5$Thesystem is entered into chaotic regime. The Lyapunov exponent is also fluctuating between two values that is negative and positive, which also suggests that the system is showing irregular cures with. It states that the system exhibits chaotic dynamics with temporary stability.

When $r \approx 4.0$Lyapunov exponent It's showing up straight spike upward suggesting a strong chaos. During this regime the system is highly sensitive towards its initial conditions even a slightest change can lead to drastic different outcomes the positive exponent in this range confirms the system is chaotic in nature with unpredictable and uncertainty dominating this region. From initial analysis we can confirm that using these two-membership functions can lead to chaos and uncertainty in the logistic map, greatly enhancing the cryptographic properties of the map.

Further analyzing the cryptographic properties of the map, we can use NIST STS test [9], which is a compressive test for analyzing the custom cryptographic methodologies and usefulness in current systems [8]. This test Firstly creating bit streams is required for this test mostly one-million-bit streams is sufficient to give the usage and valuable information regarding modified system.

The methodology we are using for generating the best stream has been discussed in [1] In which the threshold value is initially set such that when the value of the system is greater the bit is 1 and if it is less than it should be 0.

$$B_n = \begin{cases} 1 & \text{if } d_i \geq T \\ 0 & \text{if } d_i < T \end{cases}$$

B_n is the bit stream generated by the formula above.

d_i Represents the logistic map values for a particular iteration.

T It is a threshold value from which the bits of the bit stream are generated in this case the default value is set to 0.5.

The initial values of the Bitstreams have to be removed as they don't contain any uncertainty which can give us false results for the chaotic system.

During the test the test suite is version 2.1 .2 and the initial settings for the test are default that is for block frequency test the block length is set to 128, Non overlapping text block length is 9, overlapping template test block length is 9, for Approximate entropy test the block length is at 10, for serial test the block length is at 16 and for Linear complexity test the block length is set to 500.

The logistic map growth rate is at 3.99, standard deviation is set to 0.1, mean is set at 0.5 and 20 bitstream are generated of 1,000,000 bits each discarding every initial 10 bits of each bitstream.

Table No 1 NIST test result when r = 3.99

P-VALUE	PROPORTION	STATISTICAL TEST
0.637119	20/20	Frequency
0.122325	20/20	BlockFrequency
0.437274	20/20	CumulativeSums
0.911413	20/20	CumulativeSums
0.213309	20/20	Runs
0.534146	19/20	LongestRun
0.066882	20/20	Rank
0.213309	19/20	FFT
0.834308	20/20	NonOverlappingTemplate
0.437274	20/20	NonOverlappingTemplate
0.350485	20/20	OverlappingTemplate
0.834308	20/20	Universal
0.991468	18/20	ApproximateEntropy
0.911413	10/10	RandomExcursions
0.739918	10/10	RandomExcursionsVariant
0.350485	20/20	Serial
0.275709	19/20	Serial
0.739918	20/20	LinearComplexity

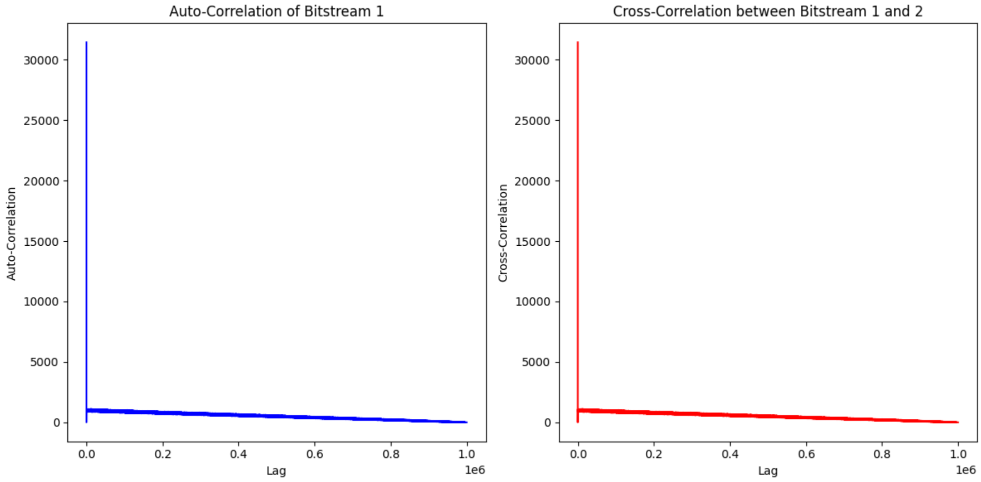

Fig No. 10 auto-correlation and cross correlation of the modified logistic map

Figure No 10 shows the Autocorrelation across correlation of the pit stream generated by the Modified logistic app. In the left the graph quota correlation in the ideal behavior shows the effective randomness and Chaos of the system which can be used in encryption the autocorrelation should resemble white noise in which the function should only have significant value at zero lakh and should be close to zero for all other lags from the graph on the left shows the sharp speak at zero lakh near zero values in others which is suggesting that the piston has low correlation values with itself over the time. Which is essentially good for encryption, and it also shows a good degree of randomness having no pattern persisted across the sequences. On the right of three figure no. 13 shows the cross correlation in the ideal encryption system the cross correlation between two different should be negligible it should be near zero which means that distance is independent statistically and doesn't have repeated patterns and doesn't share patterns. From the graph of the cross-correlation plot shows higher value at zero lags as every sequence is correlated trivially with itself at this point but the sudden sharp valley dropped near zero for other lags. From this it is suggesting that the two best shrinks are unrelated and uncorrelated which is a desirable property for encryption as the different bit stream should be uncorrelated to avoid predictability. Based on the graph we can conclude that the modified chaotic system will function well in encryption purposes in terms of randomness and independence of bitstream.

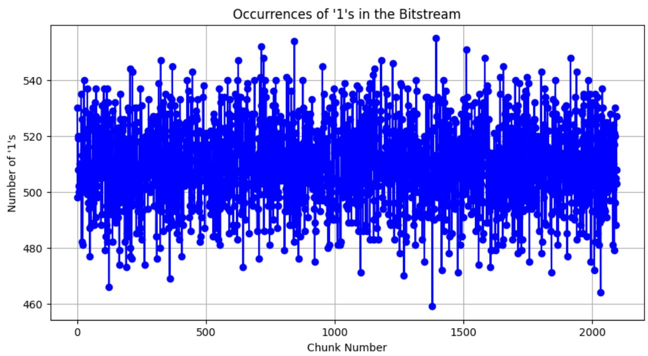

Fig No 11 occurrence of 1's in a bit stream

Above graph is illustrating the distribution of occurrence of '1's in different chunks of bit stream Generated by the modified logistic map using version membership function the graph is showing that the number of '1's In each chunk this fluctuating around the value 500 around the midpoint of the graph but it remains within a reasonable range this variation should be expected in a chaotic system where a small deviation occur, but the distribution stays balanced. The distribution in each which is a key factor that determines the randomness and Unpredictability of a bit stream in a cryptographic application a balance fluctuation shown in the graph ensures that the bit stream either should be biassed nor repetitive which are both essential properties for secure encryption.

For performing encryption using the modified logistic map which uses Gaussian membership function it has certain steps in which firstly The image is grey scared at each pixel takes a value then value is converted into binary number and is shaped into a single matrix. In second step the matrix of the original image is XORed with the bitstream Of the modified chaos system and the resultant is the encrypted sequence Which is done reconstructed into receiver hand by reversing the procedure. For the test Image use is 512x512 Image of Lena and the resultant is shown in Fig No 12

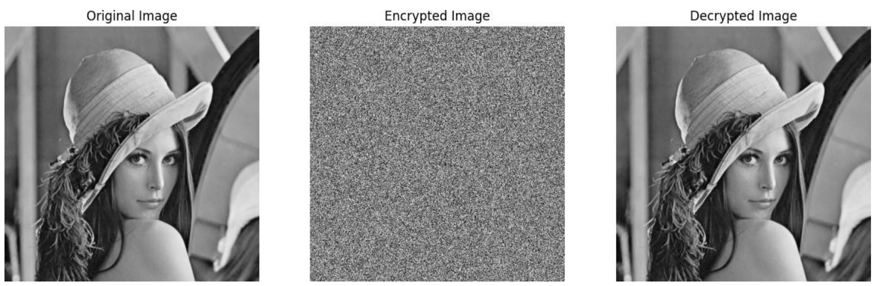

Fig No 12 performing encryption and decryption in Lena image of 512x512

Table 2 correlation coefficient of original and encrypted image

Image type	Horizontal	Vertical	Diagonal
Original	0.9721	0.9854	0.9593
Encrypted	-0.0092	-0.0096	-0.0092

The correlation coefficient values of horizontal vertical and diagonal coefficients are negative but stay close to zero the negative value is mostly likely to a result of minor random fluctuations in the data. These negative values indicate no significant correlation between original and encrypted images, which is essential of a well-designed encryption scheme. The proposed chaos system introduced randomness due to which may result a slight negative correlation between pixel pairs these situations are not indicatory of any strong linear relationship rather than artefacts of randomness which is introduced by the Gaussian membership function in the modified. In most cryptographic systems small positive or negative values are acceptable as long as overall value is near zero which simplifies randomness and a strong encryption schemes.

IV. Conclusion

Integration of complex chaotic maps could be a potential way of advancing encryption algorithms that are effective and secure. The following examinations will assess the potential for the utilization of complex chaotic systems such as multi-dimensional chaotic systems and hyperchaotic maps, to enhance the complexity and safety features of the encryption process. In these systems, potential benefits could include significantly higher resistance of the algorithm to the major cryptographic analysis methods. Further research and development are needed to adjust the chaotic parameters in the encryption process. The investigation of adaptive methods or machine learning-produced techniques may allow dynamic modification of these parameters with increased safety. By the continued enhancement of chaotic parameters, evolving threats can be mitigated.

The integration of hybrid encryption schemes is one avenue that researchers could pursue. The combination of chaotic maps and other cryptographic methods (for instance, quantum cryptography or homomorphic encryption) might be able to create hybrid systems that surpass other security models based on both security and performance. These hybrid systems are expected to address the limitations of single chaotic map usage and thus represent a more effective and efficient encryption approach.

Selective encryption is another area in this context that has good prospects. Through the use of chaos-based mechanisms for partial image encryption, a decrease in computational load while still maintaining higher security levels is achievable. This method can be particularly significant in real-time application situations where a high speed of processing is necessary.

Proper security analysis and cryptanalysis of the proposed chaotic encryption algorithms are very important to recognize probable vulnerabilities at the very beginning. The abstraction of these features of these functions by using a library could help reduce the code size as well as simplify the calling process.

The growth of the computational efficiency of chaotic encryption algorithms is another area that has to be pursued in future research. Optimization methods for devices, i.e., GPUs (Graphics Processing Units) or FPGAs (Field Programmable Gate Arrays), as well as parallel processing exploration, will be key to improving these algorithms in real-world applications.

Expanding the paradigms of encryption techniques to other non-image forms such as video, audio, or text can be a very interesting extension. The next research work will delve into the necessary modifications and challenges in the context of the efficient encryption and decryption of different information types.

The actual application of chaotic encryption algorithms on existing communication systems, their size, and adaptability is going to be the real-world testing technique. The initial step will be to verify the initial state of the data transfer system, followed by the scalable confirmation of the successful transfer.

Also, the idea of user-defined chaotic systems seems to be a source of discovery in prospective research studies. This includes the prospective checking of the increased security feature during transmission, utilization, and archival of cloud data.

References

[1] Moysis, L., Volos, C., Jafari, S., Munoz-Pacheco, J. M., Kengne, J., Rajagopal, K., & Stouboulos, I. (2020). Modification of the Logistic Map Using Fuzzy Numbers with Application to Pseudorandom Number Generation and Image Encryption. Entropy, 22(4), 474. https://doi.org/10.3390/e22040474

[2] Gad, M., Hagras, E., Soliman, H., & Hikal, N. (2021). A new parallel fuzzy multi modular Chaotic Logistic map for image encryption. The International Arab Journal of Information Technology, 18(2). https://doi.org/10.34028/iajit/18/2/12

[3] Fradkov, A.L.; Evans, R.J. Control of chaos: Methods and applications in engineering. Annu. Rev. Control. 2005, 29, 33–56

[4] Wu, G.C.; Baleanu, D. Discrete fractional logistic map and its chaos. Nonlinear Dyn. 2014, 75, 283–287.

[5] Han, C. An image encryption algorithm based on modified logistic chaotic map. Optik 2019, 181, 779–785.

[6] Chen, S.L.; Hwang, T.; Lin, W.W. Randomness enhancement using digitalized modified logistic map. IEEE Trans. Circuits Syst. II Express Briefs 2010, 57, 996–1000.

[7] Li, Z., & Chen, G. (2010). Integration of Fuzzy Logic and Chaos Theory.https://doi.org/10.1007/3-540-32502-6.

[8] Patidar, V.; Sud, K.K.; Pareek, N.K. A pseudo random bit generator based on chaotic logistic map and its statistical testing. Informatica 2009, 33, 441–452.

[9] Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E. A statistical Test Suite for Random and Pseudorandom Number Generators for cRyptographic Applications; Technical Report; Booz-Allen and Hamilton Inc.: Mclean, VA, USA, 2001.

[10] Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurc. Chaos 2006, 16, 2129–2151.

[11] Andrecut, M. Logistic map as a random number generator. Int. J. Mod. Phys. B 1998, 12, 921–930.