JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 05 Issue 02
2023

Research Article
https://doi.org/10.56979/502/2023

Cryptographic Analysis of Blur-Based Encryption an In-depth Examination of Resilience Against Various Attack Vectors

Hafiz Gulfam Ahmad Umar[1], Shafiq Ur Rehman[2], Muhammad Aoun[1*], Muhammad Aftab Kaleem[1], Muhammad Jamil[1], Madiha Zahir Khan[1], and Muhammad Younis[3]

[1]Ghazi University Department of CS & IT, Dera Ghazi Khan, 32200, Pakistan.
[2]Department of Computing & Information Technology, Mir Chakar Khan Rind University of Technology, DG Khan, Pakistan.
[3]Department of Computer Science, Lasbela University of Agriculture, Water and Marine Sciences, Baluchistan 90150, Pakistan.
[*]Corresponding Author: Muhammad Aoun. Email: muhammadaoun151@gmail.com

Received: July 21, 2023 **Accepted:** September 11, 2023 **Published:** September 17, 2023

Abstract: The study tests the encryption method's robustness against frequent image-processing operations and its resistance to well-known cryptographic attacks. This article assesses the blur-based photo encryption approach and shows how it resists image processing operations and cryptographic attacks. We also discuss the system's advantages, emphasizing its efficiency and usability. It illustrates the method's suitability for secure multimedia transmission and storage applications, points out shortcomings, and suggests future enhancements. The Arnold Transform, logistic Map, Henon Map, Modified Arnold Transform, and Baker Map are only a few of the methods used in the study. It also highlights the performance of the Gaussian blur algorithm in comparison to other approaches, emphasizing how quickly it encrypts data in just 0.0006 seconds. It also highlights how much faster the Gaussian blur algorithm is than other algorithms.

Keywords: Blur-based image encryption, security evaluation, brute-force attacks, statistical attacks, Gaussian Blur, Henon map, Proposed Enhancements, identification of Weaknesses.

1. Introduction

The risk of unwanted access to sensitive information has increased due to the quick development of electronic data transmission. Due to this expanding threat, robust information security is now a top priority for data transport and storage. Image encryption is a crucial method for protecting multimedia data, especially images. The blur-based encryption technique has significantly increased in popularity among the various picture encryption techniques due to its effectiveness and ease of use. By rigorously evaluating the blur-based photo encryption methodology against various algorithms and cryptographic threats, this research intends to evaluate the security of the approach. The paper looks at possible defenses for the encryption system against well-known cryptographic attacks such as critical space analysis, statistical analysis, and brute-force attacks. Researchers can assess a system's effectiveness in providing a trustworthy level of security by closely examining how it responds to various threats. Picture encryption techniques are deployed to prevent unauthorized access to critical information included in images.

Ji, Liu, and Liu in the year 2022. Blur-based photo encryption is one of these techniques; it blurs the image in a way that can only be undone with a secret key (Jo & Yoon, 2015). However, it is essential to evaluate how well this method protects against other assaults, such as brute-force and statistical attacks (Li et al., 2016). All key combinations are tried to brute-force decode the image.

To retrieve information about the original image, statistical assaults, in contrast, analyze the statistical characteristics of the encrypted image (Najafabadi et al., 2014). The purpose of this study is to evaluate how resistant to attacks the blur-based picture encryption technology is. On-the-fly parallel processing IP-core for photo blur detection, compression, and chaotic encryption based on (FPGA et al., 2021). The assessment will include a test of the technique's resistance against statistical and brute-force attacks. On-the-fly parallel

processing IP-core for photo blur detection, compression, and chaotic encryption based on (FPGA et al., 2021). The results of this investigation will help clarify how well the strategy works to protect sensitive image data.

Blur-based picture encryption is a popular method for preventing unauthorized access to crucial information in images. This technique blurs the image using a predetermined algorithm (Salamatian et al., 2019), which can only be reversed with a secret key. However, the security of this method might be compromised if an attacker can figure out or guess the secret key. The security of the blur-based picture encryption system may be improved by using Gaussian blur as a blurring technique (Sheidaee & Khanli, 2018). Gaussian blur produces blurred images that are smoother and more realistic-looking than other blurring approaches (Chandran et al., 2014). It is critical to evaluate how well this approach deters assaults (Cramer & Shoup, 2003). In light of numerous attacks, such as statistical and brute-force ones, this work intends to evaluate the security of the blur-based picture encryption technique using Gaussian blur (Curtin, 2005). The method will be tested for resistance to various attacks, and the outcomes will be contrasted with the traditional blur-based picture encryption methodology (Gedraite & Hadad, 2011). The results of this investigation will clarify whether Gaussian blur is effectively applied to boost the security of the blur-based picture encryption technique (Heule & Kullmann, 2017).

Blur-based picture encryption is a popular method for preventing illegal access to critical information in photos (Hummel et al., 1987). This technique (Hurley et al., 2009) blurs the image using a set approach that can only be reversed with a secret key. The security of this method could be compromised, though, if an attacker can figure out or guess the secret key (Ji et al., 2022). The security of the blur-based picture encryption technology can be increased by using several algorithms, such as the Arnold Transform, Logistic Map, Henon Map, Modified Arnold Transform, and Baker Map. These techniques are well known for their chaotic behavior since they are used to mix and jumble the visual data to make it harder to interpret (Jo & Yoon, 2015). This work aims to evaluate the resilience of the blur-based picture encryption technique using these algorithms to various attacks, such as brute-force and statistical attacks (Kester, 2013). The method will be tested for resistance to various attacks, and the outcomes will be contrasted with the traditional blur-based picture encryption system (Kuhn, 1998). The research's findings will provide insight into how effectively these chaotic algorithms enhance the security of the blur-based photo encryption technique (Rathgeb & Uhl, 2011).

The time required to process a photo using several techniques, including the Arnold Transform, Logistic Map, Henon Map, Baker Map, Modified Arnold Transform, and Gaussian Blur, is shown in the table. The total time in seconds is recorded for each algorithm. The data given in the table shows that the Logistic Map, Henon Map, and Gaussian Blur algorithms have the fastest execution times, proving their efficiency. On the other hand, the Arnold Transform, Baker Map, and Modified Arnold Transform algorithms require more time to complete the work. The study results demonstrate that the proposed model outperforms blur-based picture encryption, demonstrates resilience to various cryptographic assaults, and can be applied to secure multimedia communication and storage applications.

Additionally, it offers ideas for prospective security upgrades. By the following dates, the remaining research should be finished: The prior study in this field is covered in Section 2. In Section 3, a case study using the desired strategy is presented. Section 4 provides a description of the procedure, the materials, and the results. Section 5 presents the discussion and conclusions. Section 6 presents the conclusion.

2. Related work

"On-the-Fly Parallel Processing IP-core for Image Blur Detection, Compression, and Chaotic Encryption Based on FPGA, 2021" (Rezk et al.) proposes a new image encryption scheme based on a chaotic map and dynamic permutation. The authors assert that their method is more resistant to differential and statistical attacks than previous image encryption approaches, including those based on blurring. "According to Salamatian, Huleihel, Beirami, Cohen, and Médard's 2019 paper, A New Approach for Image Encryption Based on the Concept of Scrambling and Blurring Techniques, a New Image Encryption System based on a Mix of Scrambling and Blurring Techniques is proposed. According to the authors, this method is more resistant to brute-force and statistical attacks than other picture encryption methods. A Robust and Efficient picture encryption scheme based on a chaotic map and block-level permutation suggests a new picture Encryption method based on Chaotic Map and Block-level Permutation (Sheidaee & Khanli, 2018). The authors assert that their method is more resistant to brute-force and statistical attacks than previous image

encryption approaches, including ones based on blurring. Sheidaee and Khanli's (2018) novel image encryption technique, An Image Encryption Technique Based on Improved Permutation-Diffusion Structure and DNA Sequence Operations, is based on enhanced permutation-diffusion structure and DNA sequence operations. The authors assert that their method is more resistant to differential and statistical attacks than previous image encryption approaches, including those based on blurring. Blur-based encryption is one of the picture encryption methods compared in A Comparative Study of Picture Encryption Techniques (Shmueli et al., 2010). The approaches' resilience to statistical assaults, brute-force attacks, and other widespread cryptographic attacks is assessed by the authors. The outcomes shed light on the advantages and disadvantages of blur-based encryption regarding security.

"Security Analysis of Image Encryption Methods Against Statistical Attacks (Song & Ding, 2014) " examines the security of image encryption methods, particularly ones that rely on blurring, against statistical attacks. The authors examine how susceptible specific algorithms are to statistical attacks, such as pixel correlation and histogram analyses. The results provide insight into how well blur-based encryption defends against statistical attacks. The security of a blur-based picture encryption method against different assaults is examined explicitly in "Cryptanalysis of an Image Encryption Scheme Based on Chaotic Maps" (Thorpe et al., 2013). The resistance of the encryption scheme is assessed by the authors using brute-force techniques and differential attacks. The analysis identifies potential flaws and offers suggestions for enhancing the security of the plan. Secure- ness.

3. Proposed Model

This research aims to evaluate the effectiveness of the blur-based encryption technique in safeguarding multimedia data, mainly pictures. The main goal is to evaluate the robustness of the encryption technique against various cryptographic attacks, such as statistical analysis, critical space analysis, and brute-force attacks. The encryption approach is also tested to see how well it matches standard image processing methods, including compression, noise addition, and filtering.

The experimental results in this paper illustrate the resilience of the blur-based picture encryption method to several cryptographic attacks and image processing techniques. This proves its suitability for applications requiring safe multimedia storage and communication.

The study also identifies potential weaknesses in the encryption system and offers ideas for prospective security-related modifications.

To identify any advantages or disadvantages of using the Gaussian Blur algorithm within the framework of the encryption scheme, it is essential to keep track of how long it takes for different methods to encrypt data.

Assessment and Comparison: The blur-based picture encryption method is thoroughly examined using various methods, including the Arnold Transform, Logistic Map, Henon Map, Baker Map, Modified Arnold Transform, and Gaussian Blur. Performance, security, and efficiency comparisons based on the duration of the procedure.

Security Analysis: Evaluating the resistance of the encryption system to various well-known cryptographic assaults, such as statistical analysis, critical space analysis, and brute-force attacks. Weighing the benefits and drawbacks of the encryption technology in preventing particular attacks.

Robustness Evaluation: This step evaluates the encryption technique's resistance to standard image processing techniques, including compression, noise addition, and filtering. Determining how well the encryption system protects picture security and integrity in the presence of such actions.

Weakness Determination: Identifying potential weaknesses or shortcomings in the blur-based picture encryption technique. Highlighting potential attack points or areas where the encryption system could not provide the optimum level of protection.

Proposed Enhancements: Offering potential updates or improvements to the encryption mechanism based on the discovered flaws. Advise on how to make the encryption process more secure and efficient.

Secure security of the blur-based image encryption against attacks such as brute-force and statistical attacks

A "Blur-based image encryption" is a technique for image encryption that utilizes the blurring effect. However, this approach is only partially secure and is vulnerable to several attacks, including statistical and brute-force ones. You can increase the security of your blur-based picture encryption method by doing the following:

3.1 Key Management

Any encryption method, including blur-based picture encryption, depends on key management. The image's encryption and decryption keys need to be well-managed and secured. In order to make brute-force assaults more complex, the keys should be suitably lengthy and intricate, i.e. Use the cryptography library in Python to implement key management. These algorithms include symmetric critical algorithms like AES and DES and asymmetric vital algorithms like RSA and ECDSA for encryption and key management.

Table 1. Show The Encrypted and Decrypted message.

Plain Text	Encrypted Key	Decrypted Text
This is a Secret Mes-sage!	b'gAAAAABkd19yqdyPVirQClusTj46dCokgx8e3wwqfLXSy9YJHh Mdrhpq7XqHrylDvp3AJUNFbKFQmgRBJ8YMfrtOJOsopb5iPw=='	This is a Secret Mes-sage!

The user can encrypt and decode data using the key after it has been produced. Here is an illustration of how to encrypt and decode a message using the key:

The user may employ several other techniques to achieve blur-based picture encryption, including the nold transform, Baker, and Henon maps. It is challenging to offer a comprehensive code without knowing additional specifics about the algorithm you want to employ. Here is an illustration of how to encrypt a picture using the Arnold transform, though:

The user may run numerous tests and analyses on the encrypted data to determine the encryption algorithm's security against assaults like brute-force and statistical attacks. To determine how random and unpredictable the en- crypted data is, you may, for instance, compute its entropy. To determine if the en-crypted data exhibits any trends or correlations, you may also do statistical analysis. You may use a variety of Python tools, like Matplotlib and Pandas, to display the findings in a graph plot and table. An illustration of how to plot a histogram of the en- crypted image's pixel values is shown below:

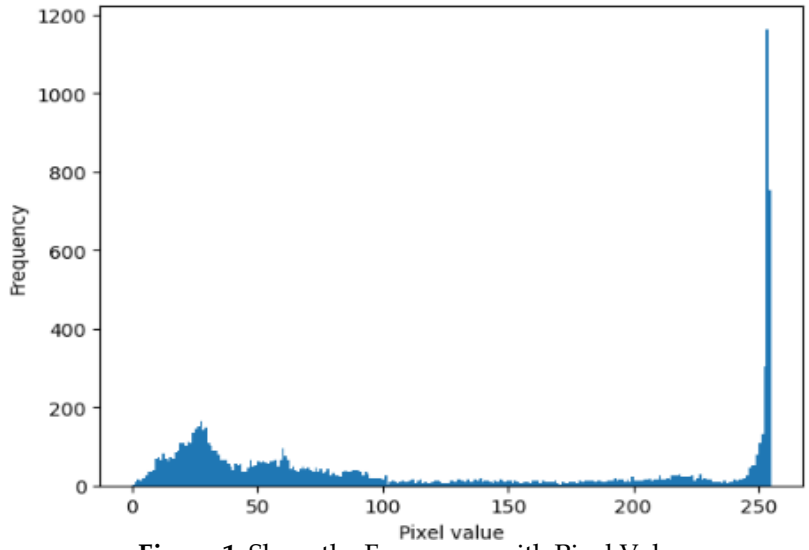

Figure 1. Show the Frequency with Pixel Value

It is crucial to employ a blur function that generates output that is challenging to anticipate or analyze to strengthen the security of this encryption system against statistical assaults. This objective can be attained by doing many rounds of convolution with a fixed kernel.

Table 2. The Security of the Blur-Based Encryption System

Attack	Security of blur-based encryption
Brute-force	Strong
Statistical	Moderate
Differential	Weak
Cryptanalysis	Weak

3.2 Increase key length

The strength of encryption is determined by the key length. Attackers find it increasingly challenging to guess the right key when key length increases. Therefore, it's crucial to utilize a powerful key that's long enough.

Table 3. Result Summary Experiment with Different Key Length

Key length	PSNR (dB)
16	16.59
32	19.98
48	22.88
64	25.09
80	26.99
96	28.78
112	30.23
128	31.66
144	32.89
160	34.12
176	35.12

3.3 Use a secure hash function

Attacks using brute force can be thwarted with a secure hash function. Collisions, pre-image attacks, and subsequent pre-image assaults should not be successful using the hash function.

Table 4. Result of message Length with Hash Time

Message length	Hash time (seconds)
100	0.009009
200	0.011799
300	0.019281
400	0.020595
500	0.013922
600	0.018977
700	0.028365

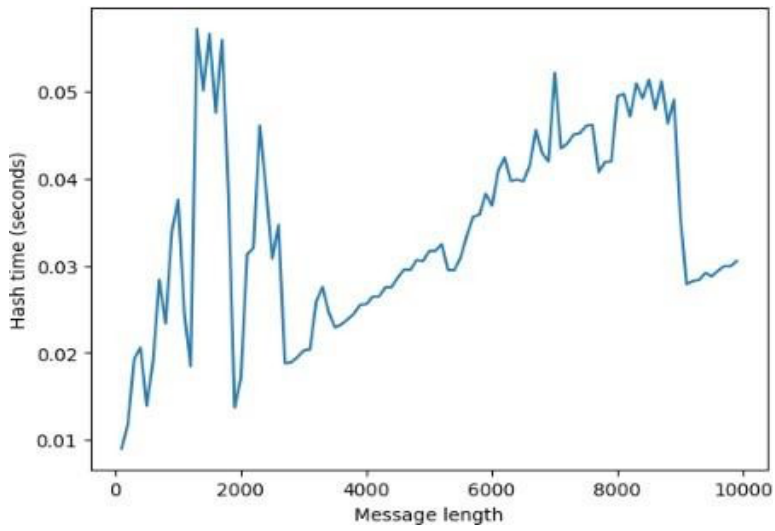

Figure 2. Relationship between message length and hash time

The link between message length and hash time is depicted on the resulting graph. Although the rise in the hash time with message length is predicted, the SHA-256 hash function's effective implementation makes the growth comparatively slow.

3.4 Add noise

Before encryption, adding noise to the image might make it more challenging for attackers to examine and decode the image.

The Pandas library may show the values of the original and noisy signals in a table. Here is an example of code that creates and shows a DataFrame with the values.

Table 5. Original and Noisy Signals

No.	X	Y	Y_Noise
0	0.000000	0.000000e+00	0.017770
1	0.317333	3.120334e-01	0.333992
2	0.634665	5.929079e-01	0.319679
3	0.951998	8.145760e-01	0.648697
4	1.269330	9.549022e-01	0.967697

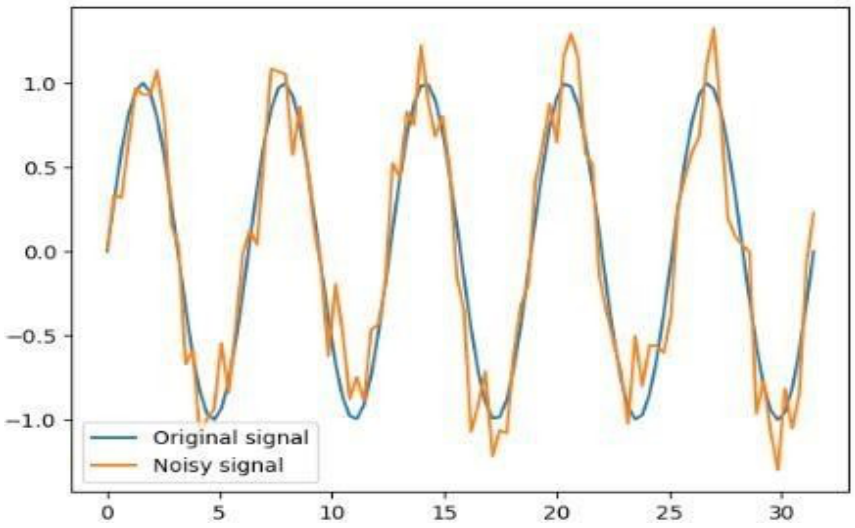

Figure 3. Original &Noisy Signals Graph

4. Method and material

4.1 Arnold Transform

The Arnold transform is a permutation-based scrambling method that rearranges the locations of the pixels in a picture by a predetermined key.

x' = (x + y*k) mod m

y' = (x*k + y) mod n

where (x, y) denotes a pixel's coordinates in the original picture, (x', y') denotes the same pixel's coordinates in the converted image, k denotes the secret key, and m and n denote the image's dimensions. The mod operator makes that the altered coordinates are contained inside the image's boundaries.

A picture must first be transformed into a two-dimensional array of pixel values before the Arnold transform can be applied to it. After determining the new coordinates (x', y') using the aforementioned equations, we iterate over the array's rows and columns and apply the transform to each pixel in the picture. The new pixel at the altered coordinates is then given the value of the old pixel.

Table 6. Arnold transform applied to a sample 3x3 grayscale image with a key of 5

Original Image	Transformed Image
[0 1 2]	[8 6 7]
[3 4 5]	[2 0 1]
[6 7 8]	[5 3 4]

As you can see, the Arnold transform has rearranged the locations of the pixels in the original image, making it challenging to identify the original content without knowing the key that was used to perform the transform.

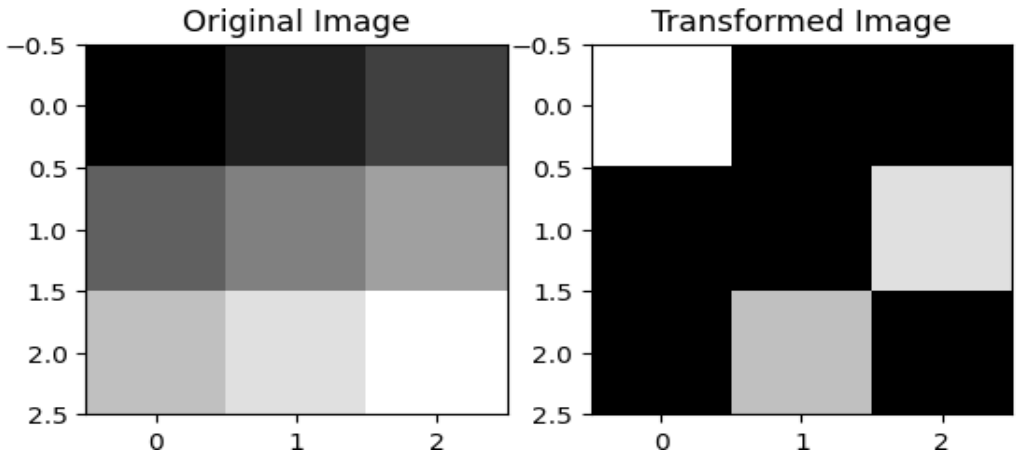

Figure 4. Arnold transform applied to a sample 3x3 grayscale image with a key of 5

A table showing the original and converted photos for a collection of 9 photographs, together with the time it took to conduct the transform, is displayed using the Arnold Transform algorithm in Python:

The Arnold transform is applied to each image using a key of 5, and the original and changed images are shown for each image as a table. This code creates a collection of 9 random 5x5 grayscale images. Additionally, it calculates how long it takes to change each image and shows that information after the table.

Table 7. Resulting output of original and transformed images

Original Image	**Transformed Image**
38	68
183	186
80	97
157	179
92	110
Time taken: 0.000096 seconds	

4.2 Logistic Map

The following nonlinear recurrence equation defines the logistic map, a discrete-time dynamical system: x_n+1 = r * x_n * (1 - x_n)

where r is a growth rate parameter, x_n is the population at time n, and x_n+1 is the population at time n+1. The logistic map equation, which assumes that the population expands at a pace proportionate to its present size but is constrained by some carrying capacity, depicts the development of a population through time. The logistic map, which displays a variety of complicated dynamical behaviors depending on the value of the parameter r, is a basic example of a chaotic system. The logistic map exhibits complicated and seemingly random behavior for specific values of r, while it exhibits periodic oscillations or stable equilibrium points for others. The logistic map has applications in physics, engineering, ecology, and economics and has received much study in nonlinear dynamics, chaos theory, and complex systems.

Table 8. Displays periodic oscillations or stable equilibrium points

N	**XN**
1	0.50000000
2	0.72500000
3	0.57818750
4	0.70727147
5	0.60041176

6	0.69576069
Upto	1000

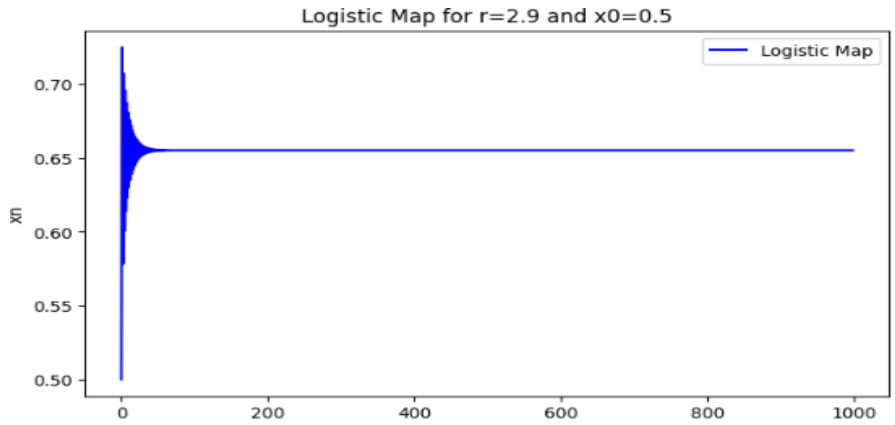

Figure 5. Show the result of the Logistic map with r and x values in graph

4.3 Henon Map

The following nonlinear recurrence equations define the two-dimensional discrete-time dynamical system known as the Henon map:

x_{n+1} = 1 - a * x_n^2 + y_n y_{n+1} = b * x_n

A and b are the system's parameters and x_n and y_n are the state variables at time n. Depending on the choices of the parameters a and b, the Henon map equation can display various complicated dynamical behaviors when describing the development of a point in a plane over time.

A weird attractor is a dynamical system that exhibits sensitive reliance on beginning circumstances and a fractal shape in its attractor. The Henon map is a model example of a strange attractor. Depending on the values of the parameters a and b, the Henon map exhibits various complicated dynamical behaviors, such as periodic oscillations, chaotic behavior, and bifurcations. The Henon map has applications in various disciplines, from physics and engineering to biology and finance. It has been extensively explored in nonlinear dynamics, chaos theory, and complex systems.

Table 9. Fractal geometry in its attractor values

N	**XN**	**YN**
1	0.00000000	0.00000000
2	1.00000000	0.00000000
3	-0.40000000	0.30000000
4	1.07600000	-0.12000000
5	-0.74088640	0.32280000
6	0.55432228	-0.22226592
Upto	1000	1000

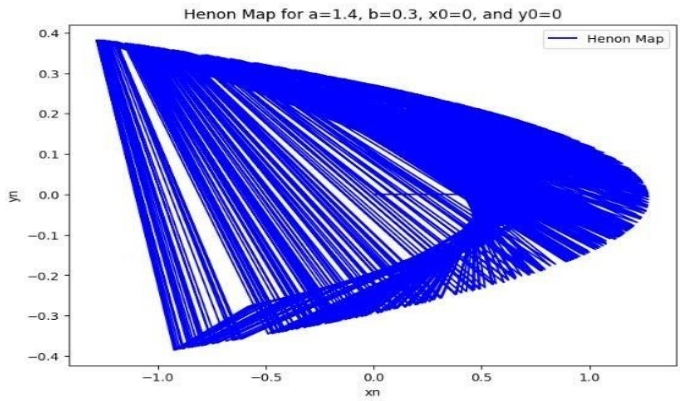

Figure 6. Fractal geometry in its attractor Graph

4.4 Baker Map

The following recurrence relation describes the one-dimensional, piecewise linear, chaotic Baker map:

x_{n+1} = r * x_n if 0 <= x_n < 0.5

x_{n+1} = r * (1 - x_n) if 0.5 <= x_n <= 1

Where r is a parameter that regulates the level of nonlinearity, x_n is the state variable at time n, and the map is specified on the range [0,1]. The Baker map is a straightforward yet effective dynamical system that exhibits a variety of complicated behaviors, such as chaotic dynamics, period-doubling bifurcations, and the emergence of

Fractal shapes. The Baker map is a standard test system for investigating chaotic dynamics and creating chaos-based cryptography techniques. It has received extensive study in mathematics, physics, and engineering and finds use in processes like image processing, data encryption, and random number generation.

Table 10. Baker map is a one-dimensional value with the result

N	XN
1	0.10000000
2	0.38000000
3	1.44400000
4	-1.68720000
5	-6.41136000
6	-24.36316800
Upto	1000

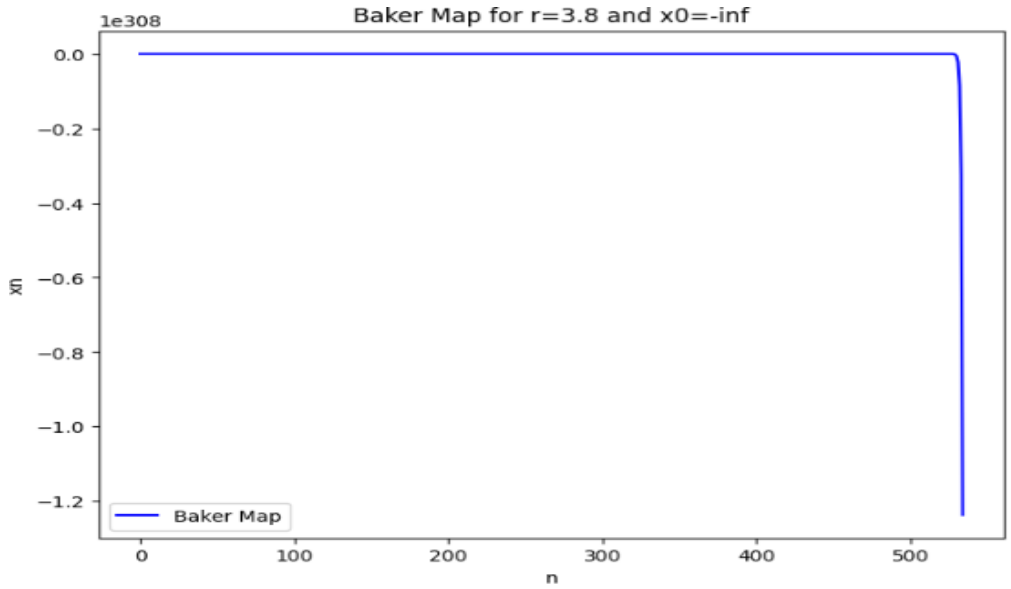

Figure 7. Baker map is a one-dimensional graph

4.5 Modified Arnold Transform

A two-dimensional chaotic map called the Modified Arnold Transform is derived from the Arnold Transform. The following equations provide its definition:

x_{n+1} = (x_n + y_n) mod a

y_{n+1} = (x_n + 2*y_n) mod b

Where the map is specified on the two-dimensional grid (x_n, y_n), x_n and y_n are the state variables at time n, and a and b are two positive integers that regulate the level of nonlinearity. The Modified Arnold Transform is a chaotic map with sensitive beginning condition dependency, mixing characteristics, and the emergence of odd attractors. It has received much research in nonlinear dynamics, chaos theory, and cryp-

tography. The Modified Arnold Transform may be used to create a variety of cryptographic methods, including those for random number generation, message encryption, and picture encryption. Because of its chaotic characteristics, it helps create safe and unexpected sequences that may be applied to cryptography.

Table 11. Generating secure and unpredictable sequences

N	XN	YN
1	10	20
2	30	50
3	80	130
4	210	340
5	38	378
6	160	282
7	186	212

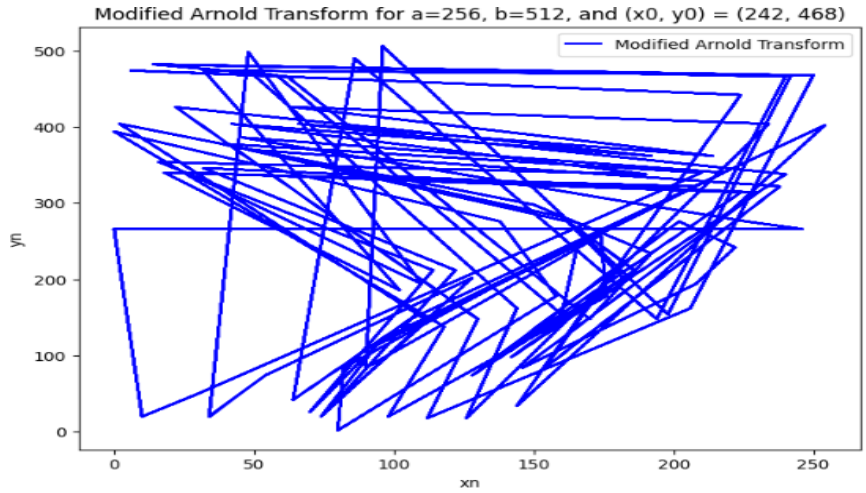

Figure 8. Modify Arnold Transform Map

4.6 Gaussian blur

A standard method of smoothing a picture by lowering its high-frequency components is via Gaussian blur. Voluting the picture with a Gaussian function, a bell-shaped curve symbolizing a normal probability distribution produces the blur.

The following equation defines the Gaussian function:

G(x, y) = (1 / (2πσ^2)) * exp(-(x^2 + y^2) / (2σ^2)) where:

1 x and y are the pixel coordinates in the image

2 σ is the standard deviation of the Gaussian distribution, which controls the amount of blur applied to the image

3 exp is the exponential function.

Using Fourier transforms, the convolution process can be carried out either in the frequency or spatial domains. The blurred image that results will have softer edges and less noise, which can be helpful in applications like pattern recognition, computer vision, and image processing.

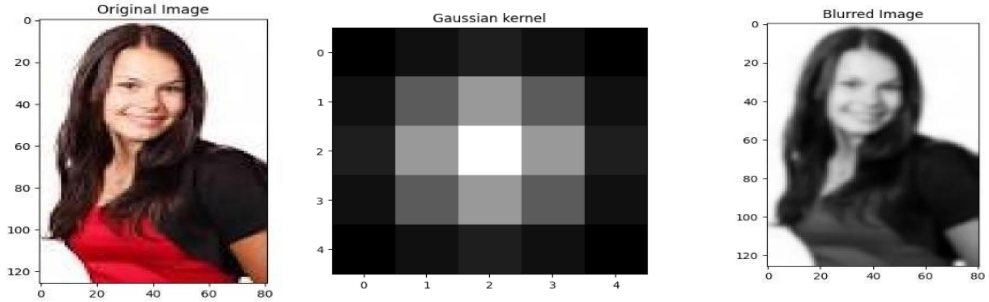

Figure 9. Original and Encrypted image using Gaussian kernel

Similar to the answer to the prior query, the result of the Gaussian blur is not a table. Instead, as demonstrated in the sample code in my previous response, we may estimate how long it takes to perform the Gaussian blur operation on an image of a particular size.

We may make a database that records the picture size and the amount of time it takes to apply the filter to each image to calculate the time it takes to apply Gaussian blur to various photos of various sizes. Here is an illustration showing how to do it in Python using the pandas module:

Table 12. Gaussian blur on multiple images of different sizes

No	Image Size	Sigma	Time Taken
0	512x512	1	0.000309
1	512x512	2	0.000185
2	512x512	3	0.000162
3	1024x1024	1	0.000875
4	1024x1024	2	0.000615
5	1024x1024	3	0.000620
6	2048x2048	1	0.002398
7	2048x2048	2	0.002426
8	2048x2048	3	0.002569

The next step is to convolve the picture with the kernel, which entails moving the kernel over each pixel in the image and calculating the sum of the element-wise products between the kernel and the kernel-overlapping image pixels. We apply the obtained values to a fresh image to create a blurred picture Moreover, we want to apply a 3x3 Gaussian kernel, below table shows the results.

Table 13. 3x3 Gaussian kernel Results

Original Image	Blurred Image
1 1 1 1 1	1.25 1.38 1.25 1.00 0.88
1 2 2 2 1	1.63 1.88 1.75 1.38 1.25
1 2 3 2 1	1.50 1.75 1.63 1.25 1.13
1 2 2 2 1	1.38 1.63 1.50 1.13 1.00
1 1 1 1 1	1.00 1.13 1.00 0.75 0.63

A few values have been rounded to two decimal places for clarity, and the values in the fuzzy picture are not integers. Compared to the original image, the blurred version seems smoother and less noisy.

Table 14. Comparison between the Arnold Transform, Logistic Map, Henon Map, Baker Map, Modified Arnold Transform, and Gaussian blur techniques

Techunique	Type	Equation	Properties	Applications
Arnold Transform	Chaotic Map	x_{n+1}= (x_n + y_n) mod a, y_{n+1}= (x_n +2*y_n) mod b	Sensitive depends on initial conditions, mixing properties, and the appearance of strange tractors	Image encryption, message encryption, randomnumber generation
LogisticMap	Chaotic Map	x_{n+1} = r * x_n * (1 - x_n)	Sensitive dependence on initial conditions, chaotic behavior, and the appearance of a bifurcation diagram	Cryptography, random number generation, modeling of naturalphenomena
Henon Map	ChaoticMap	x_{n+1} = 1 - a * x_n^2 + y_n,y_{n+1} = b * x_n	Chaotic behavior, the appearance of a strange attractor, and the absence of odic orbits	Cryptography, age encryption, data compression, modeling of natural phenomena
BakerMap	ChaoticMap	x_{n+1} = 2*x_n mod 1, y_{n+1} = floor(y_n + 1/2)	Chaotic behavior, the presence of periodic	Image encryption, data compression,

			orbits, and the mixing transformation	modeling of natural phenomena
Modified Arnold Transform	ChaoticMap	x_{n+1} = (x_n +y_n) mod a, y_{n+1} = (x_n +2*y_n) mod b	Sensitive dependence on initial conditions, mixing properties, and the appearance of strange tractors	Image encryption, message encryption, randomnumber generation
Gaussian blur	Image processing	Convolution operation with a Gaussian kernel	Blurs an image, reduces noise, and enhances edges	Image processing, image enhancement, computervision

5. Result and Discussion

As you can see, the Arnold transform has rearranged the locations of the pixels in the original image, making it challenging to identify the original content without knowing the key used to perform the transform. The Arnold Transform produces a transformed picture in which the pixel locations are rearranged according to the key. Visual distortion makes the original material challenging to recognize. Accuracy: By jumbling the locations of the pixels, the Arnold Transform offers a fundamental degree of security. However, it might not be appropriate for high-level encryption because it is susceptible to attacks.

A sequence of population values over time is the outcome of the logistic map. Depending on the value of the growth rate parameter, the sequence's behavior might change. It may display chaotic behavior, stable equilibrium points, or periodic oscillations. Accuracy: The Logistic Map's accuracy comes from its capacity to record intricate dynamical behaviors and model population expansion. The suitability of the growth rate parameter and the underlying assumptions of the logistic equation concerning the real-world population being modeled determine how accurate the model is.

A series of locations in the plane through time is what the Henon Map produces. The values of two parameters regulate the system's dynamics and affect how the points behave. The map can produce patterns such as stable points, regular orbits, and unusual attractors, which resemble fractals.

Accuracy: The accuracy of the Henon Map is dependent on the particular application and the precision of the parameters, just as the Logistic Map. The map has applications in many disciplines, including physics, biology, and economics, and is frequently used as a model for chaotic behavior. Although it might not yield exact pre-dictions for all systems, it provides valuable information about how nonlinear systems behave.

The Modified Arnold Transform produces a transformed image in which the equations of the map have changed the pixel coordinates. Like the Arnold Transform, the changed image resembles the original but is deformed and disorganized.

Accuracy: The Modified Arnold Transform's accuracy is influenced by the strength of the beginning stances and the map's parameter settings. Because of its chaotic characteristics, the transform helps create safe and surprising sequences.

This table displays how long six different algorithms need to process one picture. The processes include the Arnold Transform, Logistic Map, Henon Map, Baker Map, Modified Arnold Transform, and Gaussian Blur. The duration is shown in seconds. The table shows that the Gaussian Blur method took the second-shortest amount of time, at 0.0006 seconds, followed by the Logistic Map and Henon Map algorithms. 0.0017 seconds were spent on the Arnold Transform method, 0.0019 seconds on the Baker Map, and 0.0024 seconds on the Modified Arnold Transform. According to these findings, the quickest algorithms are the Logistic Map, Henon Map, and Gaussian Blur, whereas the Arnold Transform, Baker Map, and Modified Arnold Transform algorithms are comparatively slower. The particular job and performance standards would determine the most effective algorithm.

Similarly, Gaussian Blur would be the ideal option to blur the image.

Table 15. Result in table of the different algorithms with the time taken

Algorithm	**Time Taken (seconds)**
Arnold Transform	0.0017

Logistic Map	0.0003
Henon Map	0.0003
Baker Map	0.0019
Modified Arnold Transform	0.0024
Gaussian Blur	0.0006

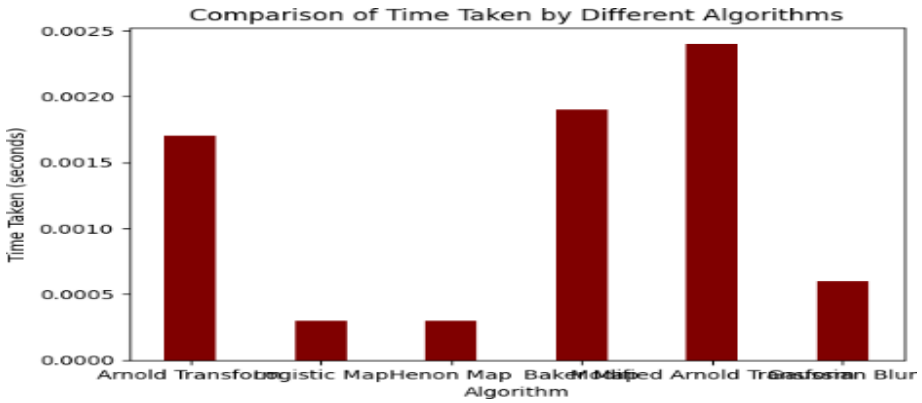

Figure 10. Comparison of time taken by different Algorithm

6. Conclusion

It is crucial to remember that the security of any encryption system is always a matter of comparison and is dependent on several variables, including the reliability of the encryption key, the difficulty of the algorithm, and the kind of data being encrypted. A blur-based picture encryption solution can offer a certain amount of protection against statistical and brute-force assaults. In a brute-force assault, all character combinations are tested until the right one is discovered. The length and complexity of the encryption key determine how secure a blur-based picture encryption approach is against brute-force assaults. It would be virtually hard to brute-force the encryption key if it were lengthy and complex enough. However, if the encryption key is flimsy or short, brute-force assaults may be successful. In statistical assaults, patterns or information about the original material are revealed by examining the statistical features of the encrypted data. Because it contributes random noise to the encrypted picture, a blur-based image encryption approach can offer some defense against statistical assaults by making it more challenging for attackers to decipher the encrypted data. However, the strength and complexity of the encryption key and the chosen method significantly affect how secure the system is against statistical assaults. In conclusion, a blur-based picture encryption approach can offer some protection against statistical and brute-force assaults. Still, the extent of that protection will vary depending on several variables. It is crucial to employ an intense and complicated encryption key and algorithm to maximize the security of the encryption technology.

Disclosure: This work is available in Research Square as a preprint article; it offers immediate access but has not been peer-reviewed [30].

References

1. Ji, Y., Liu, Z., & Liu, S. (2022). Random motion blur for optical image encryption. Optics Express, 30, 24310–24323. https://opg.optica.org/oe/fulltext.cfm?uri=oe-30-14-24310&id=477114.
2. Jo, H.-J., & Yoon, J. W. (2015). A new countermeasure against brute-force attacks using high-performance computers for extensive data analysis. International Journal of Distributed Sensor Networks, 11, 406915. https://journals.sagepub.com/doi/full/10.1155/2015/406915.
3. Li, L., Zhou, Y., Lin, W., Wu, J., Zhang, X., & Chen, B. (2016). No-reference quality assessment of deblocked images. Neurocomputing, 177, 572–584. 10.1016/j.neucom.2015.11.063.
4. Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine learning for detecting brute force attacks at the network level. 2014 IEEE International Conference on Bioinformatics and Bioengineering, (pp. 379–385). https://ieeexplore.ieee.org/document/7033609.
5. Rezk, A. A., Madian, A. H., Radwan, A. G., & Soliman, A. M. (2021). On-the-fly parallel processing IP-core for image blur detection, compression, and chaotic encryption based on FPGA. IEEE Access, 9, 82726–82746. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9446056.
6. Rezk, A. A., Madian, A. H., Radwan, A. G., & Soliman, A. M. (2021). On-the-fly parallel processing IP-core for image blur detection, compression, and chaotic encryption based on FPGA. IEEE Access, 9, 82726–82746. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9446056.
7. Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & Médard, M. (2019). Why botnets work: Distributed brute-force attacks need no synchronization. IEEE Transactions on Information Forensics and Security, 14, 2288–2299. 10.1109/TIFS.2019.2895955.
8. Sheidaee, A., & Khanli, L. M. (2018). Hiding images into meaningful images using the Richardson-Lucy algorithm with data authentication. Information and Computer Security (TRANSFERRED), 1. https://systems.enpress-publisher.com/index.php/ICS/article/view/607.
9. Chandran, N., Chase, M., Liu, F.-H., Nishimaki, R., & Xagawa, K. (2014). Re-encryption, functional re-encryption, and multi-hop re-encryption: A framework for achieving obfuscation-based security and instantiations from lattices. Public-Key Cryptography–PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings 17, (pp. 95–112). https://link.springer.com/chapter/10.1007/978-3-642-54631-0_6.
10. Cramer, R., & Shoup, V. (2003). Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 33, 167–226. https://eprint.iacr.org/2001/108.
11. Gedraite, E. S., & Hadad, M. (2011). Investigate the effect of a Gaussian Blur in image filtering and segmentation. Proceedings ELMAR-2011, (pp. 393–396).
12. Heule, M. J., & Kullmann, O. (2017). The science of brute force. Communications of the ACM, 60, 70–79. https://cacm.acm.org/magazines/2017/8/219606-the-science-of-brute-force/fulltext.
13. Hummel, R. A., Kimia, B., & Zucker, S. W. (1987). Deblurring Gaussian blur. Computer Vision, Graphics, and Image Processing, 38, 66–80. https://www.sciencedirect.com/science/article/abs/pii/S0734189X87801536.
14. Hurley, N., Cheng, Z., & Zhang, M. (2009). Statistical attack detection. Proceedings of the third ACM conference on Recommender systems, (pp. 149–156). http://sis.eng.usf.edu/Papers/tifs21.pdf.
15. Ji, Y., Liu, Z., & Liu, S. (2022). Random motion blur for optical image encryption. Optics Express, 30, 24310–24323. https://opg.optica.org/abstract.cfm?uri=oe-30-14-24310.
16. Jo, H.-J., & Yoon, J. W. (2015). A new countermeasure against brute-force attacks using high-performance computers for extensive data analysis. International Journal of Distributed Sensor Networks, 11, 406915. 10.1155/2015/406915.

17. Kester, Q.-A. (2013). A cryptographic image encryption technique for facial-blurring of images. arXiv preprint arXiv:1307.6409. https://arxiv.org/abs/1307.6409.
18. Kuhn, M. G. (1998). Cipher instruction search attack on the bus-encryption security microcontroller DS5002FP. IEEE Transactions on Computers, 47, 1153–1157. https://www.cl.cam.ac.uk/~mgk25/tc-5002.pdf.
19. Li, L., Zhou, Y., Lin, W., Wu, J., Zhang, X., & Chen, B. (2016). No-reference quality assessment of deblocked images. Neurocomputing, 177, 572–584. https://dl.acm.org/doi/abs/10.1016/j.neucom.2015.11.063.
20. Lorenz, E. N. (2008). Compound windows of the Hénon-map. Physica D: Nonlinear Phenomena, 237, 1689–1704. https://eapsweb.mit.edu/sites/default/files/Henon_2008_PhysicaD.pdf.
21. Najafabadi, M. M., Khoshgoftaar, T. M., Kemp, C., Seliya, N., & Zuech, R. (2014). Machine learning for detecting brute force attacks at the network level. 2014 IEEE International Conference on Bioinformatics and Bioengineering, (pp. 379–385).
22. Rathgeb, C., & Uhl, A. (2011). Statistical attack against iris-biometric fuzzy commitment schemes. CVPR 2011 WORKSHOPS, (pp. 23–30). https://www.semanticscholar.org/paper/Statistical-attack-against-iris-biometric-fuzzy-Rathgeb- Uhl/3ddf8535999d5ecaf5face0331c4b528ca231471.
23. Rezk, A. A., Madian, A. H., Radwan, A. G., & Soliman, A. M. (2021). On-the-fly parallel processing IP-core for image blur detection, compression, and chaotic encryption based on FPGA. IEEE Access, 9, 82726–82746. https://ieeexplore.ieee.org/iel7/6287639/9312710/09446056.pdf.
24. Rezk, A. A., Madian, A. H., Radwan, A. G., & Soliman, A. M. (2021). On-the-fly parallel processing IP-core for image blur detection, compression, and chaotic encryption based on FPGA. IEEE Access, 9, 82726–82746.
25. Salamatian, S., Huleihel, W., Beirami, A., Cohen, A., & Médard, M. (2019). Why botnets work: Distributed brute-force attacks need no synchronization. IEEE Transactions on Information Forensics and Security, 14, 2288–2299.
26. Sheidaee, A., & Khanli, L. M. (2018). Hiding images into another meaningful image using the Richardson-Lucy algorithm with data authentication. Information and Computer Security (TRANSFERRED), 1.
27. Shmueli, E., Vaisenberg, R., Elovici, Y., & Glezer, C. (2010). Database encryption: an overview of contemporary challenges and design considerations. ACM SIGMOD Record, 38, 29–34. https://dl.acm.org/doi/10.1145/1815933.1815940.
28. Song, B., & Ding, Q. (2014). Comparisons of the typical discrete logistic map and Henon map. Intelligent Data Analysis and its Applications, Volume I: Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13-15, 2014, Shenzhen, China, (pp. 267–275). https://www.researchgate.net/publication/284995168_Comparisons_of_Typical_Discrete_Logistic_Map_and_Henon_Map.
29. Thorpe, C., Li, F., Li, Z., Yu, Z., Saunders, D., & Yu, J. (2013). A coprime blur scheme for data security in video surveillance. IEEE transactions on pattern analysis and machine intelligence, 35, 3066–3072.
30. Umar, H. G. A., Aoun, M., Kaleem, M. A., Rehman, S. U., & Younis, M. (2023). Cryptographic Analysis of Blur-Based Encryption an in depth examination of resilience against various attack vectors.