A new image encryption algorithm with a non-existent chaotic map

Ronda Priyatham
Harshita Samala
Bhetalam Vageesh
Dr. Anil Vithalrao Turukmane
Vellore Institute of technology

ABSTRACT:

In the modern era, people are more willing to utilize visual information in healthcare and military applications as science and technology are evolving. Access to such privileged data can be a dangerous threat in the modern digital age. An appropriate solution for these issues is image encryption. For image encryption, the regular text encryption techniques are not effective because the all pixel data is much larger than a regular string message and the high correlation among the adjacent pixels. So for image encryption, special techniques have to be developed to maintain the security standards, and chaotic systems are one such technique to ensure the high security standards. This study suggests an image encryption technique utilizing a 3D chaotic map. According to studies and research, this approach is more efficient and works well with image encryption.

Keywords: Image encryption, Image decryption, Chaotic map.

1.Introduction:

With the advancement of technology, our privacy becomes more transparent and threatened. Technology advancement has also improved visual communications and increased the need for visual communication in military, medical, and industrial fields. As a result, visual communications security standards must be raised to the same level as textual communications security standards. There are many text encryption techniques, such as DES and IDEA, but these algorithms do not suit the image encryption because of the data's size and strong connection between the adjacent pixels. Hence, there is a necessity for the development of secure techniques for safe visual communication. If image information is not properly processed before image transmission, there might be a danger of privacy exposure. Scientists have vigorously developed a new scientific term, "chaos," since its emergence in the 1970s. It is widely used in the cryptography field because of the nature of its randomness and its non-linearity. Because of their nature of high sensitivity to initial data, chaotic maps ensure the randomness of the generated keys. As a result, researchers began to investigate various types of chaotic maps in order to improve encryption techniques. As a result, studies have shown that continuous chaotic maps, which have a high level of complexity in general, generate low-level chaotic sequences, whereas discrete chaotic maps, despite having a low level of complexity, generate high-level chaotic sequences. Therefore, utilizing discrete chaotic maps for image encryption algorithms is more feasible. The image encryption algorithm should be clear and straightforward and keys should be secure against unwanted access, according to accepted norms. In order to satisfy all the requirements, the key generation mechanism for the algorithm must be effective. Using chaotic maps for the key generation will satisfy this need.

The general characteristics of a chaotic map are:

- The unpredictability of the keys generated by chaotic maps should be extremely complex and hard to forecast and evaluate.

- Sensitivity to the initial conditions must guarantee that even a tiny change in the initial conditions results in the generation of a completely new sequence.
- The sensitivity of the extra parameters should guarantee that even a minor alteration in the parameters must result in a completely different sequence.

If all the above conditions are met, then one cannot decrypt the image if the initial values aren't known exactly. Thus, the keys are the initial conditions in the encryption stage, and those must be shared only with the authorized persons. The study by Xiaoling Huang [1] refers to the usage of a chaotic Chebyshev map to generate a sequence that is then used as indices to scramble the positions of the pixels in a image. The scrambling technique can be useful again to shuffle the image pixels in such a way that it isn't clear to read them visually. In the study by Alireza A. Arab [3], it refers to a map with a combination of a henon map and a logistic map. This resulted in a hyperchaotic map. In a study by a Japanese researcher, T. Habutsu, he describes the iterative approach of chaotic ciphers, which was a major breakthrough in the image encryption field. research by Xingyuan Wang [4], a new two-dimensional discrete chaotic map was created to produce a large number of S-boxes, which were then dynamically used for image encryption. In the research work done by Hailan Pan [5] in this paper the the usage of two chaotic sequence generators have been implemented for both encryption and decryption. As a result, this study develops a clear and adaptable encryption technique that uses chaotic sequences and scrambling for the encryption. A brilliant property of the work is that it used the two steps in encryption, which are scrambling and chaotic sequence. The chaotic sequence generated by the map will be used for the XOR step. This proposed technique ensures all the required properties, like high sensitivity to parameters and initial conditions, and simple yet high-quality encryption and decryption.

2. Literature survey:

The use of chaotic maps in image encryption prompts the usage of mathematical algorithms to encrypt the original images, which are hard to interpret. This increases the resistance against the most commonly used security attacks, like brute force and differential attacks. The existing

algorithms on image encryptions such as [5] were derived from the existing chaotic maps and improved for better results. There are several research works done for image encryption, such as using henon maps [7] and logistic maps [8], and these works have proved great resistance against differential attacks. In most of the papers, the key systems generated by the algorithm were fixed since the initial conditions were already specified in the work by the researchers to obtain the best encryption standards and better NPCR and UACI values. This reduces the versatility to fit in different conditions, as the keys were already fixed by the researcher. In this paper, the effective way to counter this flaw will be discussed. The way to tackle this limitation is to prompt the user to enter the initial conditions for the system on which the keys are going to be generated to encrypt the image. These three initial conditions for the proposed algorithm act as keys that can be passed on to authorized users who can only decrypt the image. This ensures that every unique user can have a unique key set to encrypt the image, which maintains the confidentiality of the data since the keys differ from user to user.

3. Proposed algorithm of encryption:

In this section, the proposed algorithm will be discussed.

2.1. Chaotic map

The chaotic system equations are mentioned in Eqs. (1), (2) and (3)

$$Xn = (r^2 * (Y_{(n-1)}^2 - 5) * (1 - r * (Z_{(n-1)}^2 - 5)))\%1 \quad (1)$$

$$Yn = (r^2 * (Z_{(n-1)}^2 - 5) * (1 - r * (X_{(n-1)}^2 - 5)))\%1 \quad (2)$$

$$Zn = (r^2 * (X_{(n-1)}^2 - 5) * (1 - r * (Y_{(n-1)}^2 - 5)))\%1 \quad (3)$$

The initial values of the system used here are:

x[0]=0.2893782

y[0]=0.2819832

z[0]=0.90283982

And r is given as 1.5.

3.2. Encryption Algorithm:

- First step: convert the image to a grayscale image. A 256x256 image has been passed to the encryption algorithm.
- Second step: Now, traversing from top left to bottom right, the image will go through the scrambling process at each pixel level.

  Scrambling technique:
  - First round: Traversing from left to right row-wise replace every even ith pixel with (n-i+1)th pixel.
  - Second round: Traversing from top to bottom column-wise replace every even ith pixel with (n-i+1)th pixel.

- Third step: Now input the initial conditions to the chaotic map and generate the keys required up to N*N+1 keys, where N is the size of the image.
- Fourth step: get all the gray values of pixel decimals and store them in an array
- Fifth step: initialize a variable sum to 0.

$$sum = 0$$

- Sixth step: set i=0 j=0 and traverse through the 2D array of pixel values while

sum = sum + pixel[i][j]

And find

$$var = floor(mod(\frac{sum}{256^5}) * X(i) * 10\text{^}23, 256))$$

Now var will be in the range 0 to 255.

- Seventh step: calculate variable xkey as

xkey = 10^23 * |X(i)|

- Eighth step: Calculate the pixelKey as

  pixelKey = floorMod(xkey, 256)

- Ninth step: perform the XOR operation of pixelKey with the current gray value of pixel. and replace the pixel value with the new value obtained.

  Pixel = pixel ⊗ pixelKey ⊗ var

- Tenth step: Repeat the operation until the last pixel is reached, then return the image

Decryption algorithm:

For decryption, perform the steps mentioned in the above process to generate the key sequence.

- After generating the key sequence compute the sum as

  sum = sum + pixel[i][j]

  While traversing through the 2D array.

  Reduce the sum at each pixel by its value and goto next step.

- Calculate the variables var, xkey, and pixelKey as mentioned in the above process, and perform the XOR operation as

  Pixel = pixel ⊗ pixelKey ⊗ var

- Perform this operation until the last pixel is reached, and you will obtain a scrambled image.
- For descrambling the image, apply the reverse process of the scrambling algorithm used in the encryption algorithm.

4. Security analysis:

The number of pixels at every gray level of a picture is displayed through this histogram analysis. We'll examine different picture histograms both before and after encryption for this analysis.

Fig. 1. Photographer image

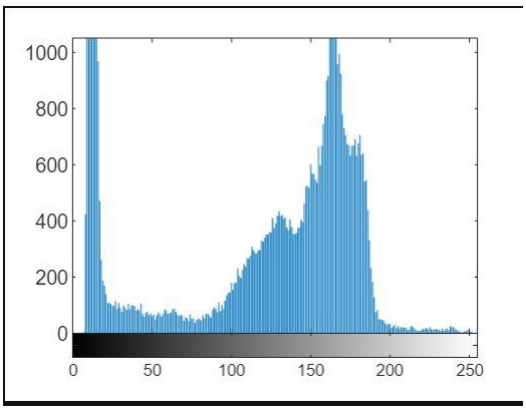


Fig. 2. Histogram of the photographer Img

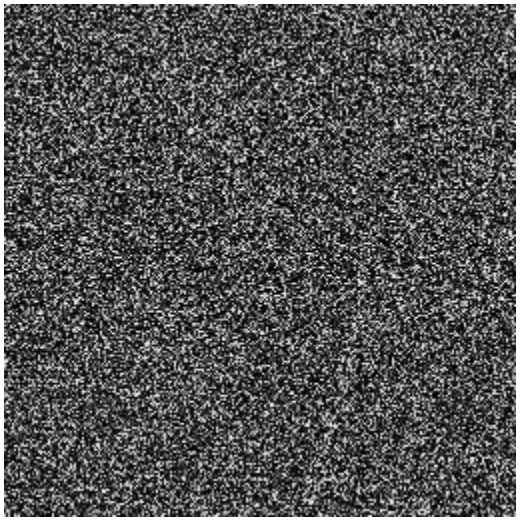


Fig. 3. Encrypted image

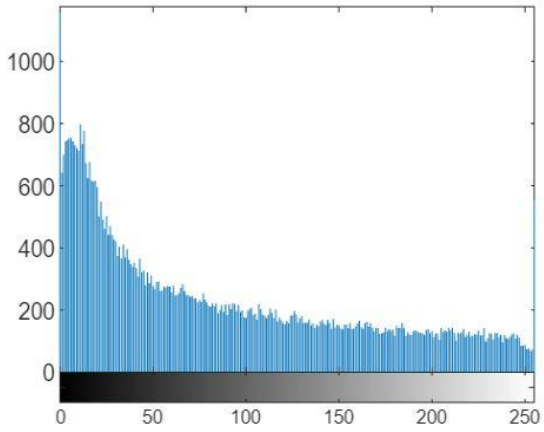


Fig. 4 Histogram of encrypted image

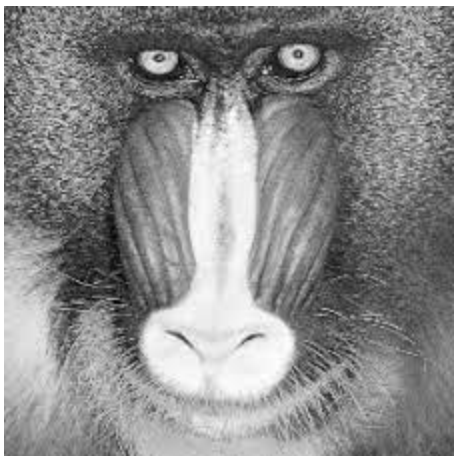


Fig. 5. Baboon original

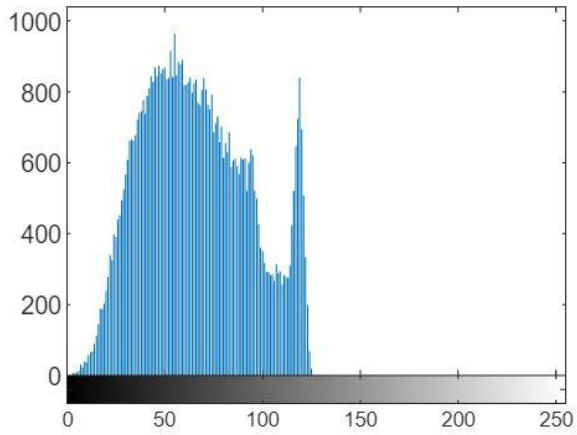


Fig. 6. Histogram of baboon

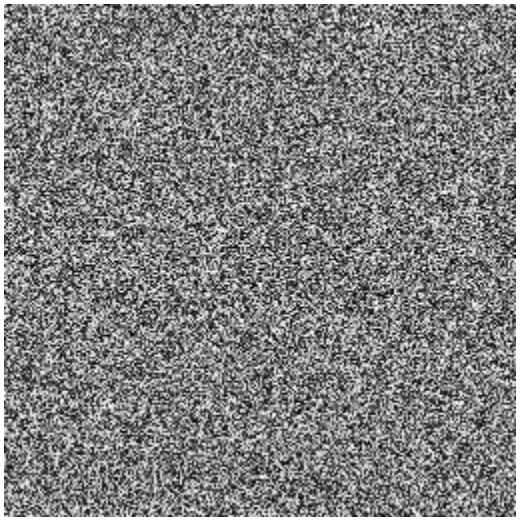


Fig. 7 Encrypted image

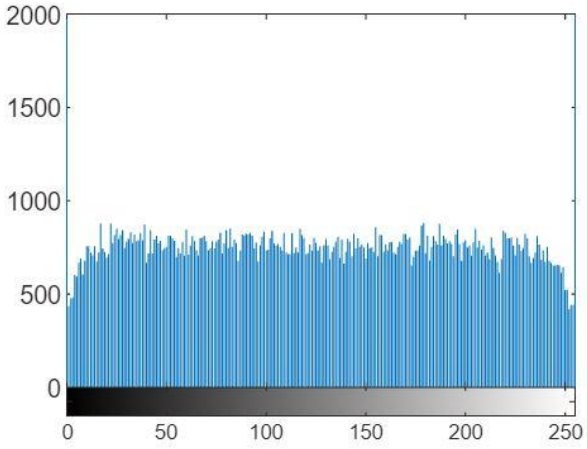


Fig. 8 Histogram of encrypted image

As seen in Fig. 4, the histogram of the encrypted picture is evenly distributed and totally distinct from the histogram of the original image. The histogram of the encrypted picture in the instance of the baboon image is more evenly distributed than the histogram of the original image.

Evaluating the sensitivity of algorithm:

To check for the sensitivity of this algorithm, a duplicate image is generated by changing one random pixel, and now we encrypt both images using the algorithm and check for the NPCR and UACI values.

UACI is the average illuminance intensity difference between these two obtained images by the equation:

$$UACI = \frac{1}{M \times N}\left[\frac{\sum i,j\left|C_{1(i,j)} - C_{2(i,j)}\right|}{2^{l} - 1}\right] \times 100$$

Where M,N are the dimensions of the image

NPCR value refers to the average number of pixels changed in the both encrypted image due to change of one pixel in the original image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$$

Where M,N are the dimensions of the image

Table.1 compares NPCR values for the proposed approach with the traditional AES technique. The table.2 compares the UACI values between the proposed technique and the traditional AES algorithm.

Table1

NPCR values (for various images)

NPCR	Lena	Baboon	Pepper	Average
AES	0.0778	0.0885	0.0885	0.0849
proposed	93.8893	93.8601	93.8992	93.8828

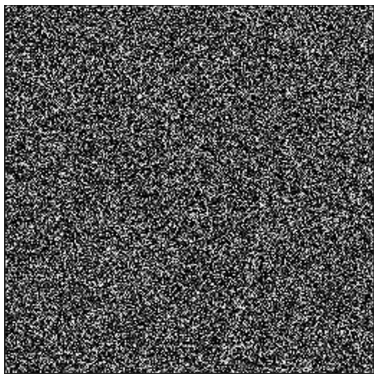
Table 2
UACI values (for various images)

UACI	Lena	Baboon	pepper	average
AES	0.0093	0.0101	0.0148	0.0114
proposed	37.8723	37.6573	37.8282	37.7859

The limit of the NPCR value is [0,100]. The nearer the obtained value of NPCR is to 100, the stronger the algorithm will be against differential attacks. The value here is closer to 100 and better than that of the AES system. UACI's desired value is 34, and the obtained value of 37 is closer to that of the AES system's UACI value. By the comparison of the UACI and NPCR values along with the histogram analysis,it can be said that the proposed algorithm has fulfilled the requirement for security against differential attack with acceptable values in UACI and NPCR.

Results:

This study proposed an algorithm that enables the user to have a unique key set to encrypt the images and maintain confidentiality and security. The proposed algorithm is highly sensitive to changes in the initial conditions.



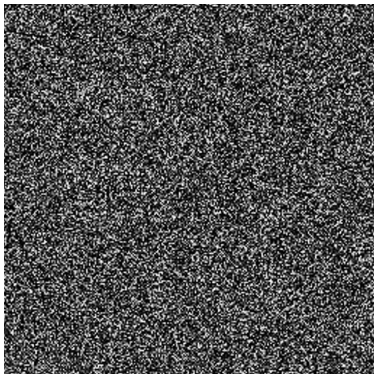


Fig. 9 Cameraman image **Fig. 10 encrypted image** **Fig. 11 decrypted image**

In the above case, fig. 11 was produced when there was a 10-12% error in one of the three keys. This demonstrates the suggested system's sensitivity to even a slight alteration in the value of its keys. This ensures the security of the image will never be compromised. Although the proposed algorithm faces a 5–10% data loss (Fig. 12), which would be corrected in a future study.

Fig. 12

Conclusion:

This paper presents the key system built using the proposed map along with an efficient scrambling tehcnique. Simulation experiments show that the algorithm is effective and indicate that it is stronger than the AES standard algorithm in terms of resistance to typical brute force and differential attacks. The crypto techniques have to evolve with time because as the tehcnology advances, so will the attack techniques. Hence the future improvements will be made.

Future Work:

Future research will focus on preventing data loss and improving the first part of the encryption's scrambling algorithm. Future study will, if at all possible, attempt to incorporate a hyperchaotic map to improve the encryption and work on video encryption based on this algorithm but with a better time complexity.

References:

[1] Xiaoling Huang. Image encryption algorithm using chaotic chebyshev generator. Nonlinear Dynamics, 67(4):2411–2417, 2012.

[2] T. Habutsu, Y. Nishio, I. Sasase, et al., A secret key cryptosystem by iterating a chaotic map[C]// the workshop on advances in cryptology-Eurocrypt. Springer-Verlag, 13(1),1-5 (1991)

[3] Alireza A. Arab, Mohammad Javad B. Rostami, Behnam Ghavami.An image encryption algorithm using the combination of chaotic maps, optik 261:169122

[4] Novel Image Cryptosystem Based on New 2D Hyperchaotic Map and Dynamical Chaotic S-box | Research Square

[5] Hailan Pan, Yongmei Lei & Chen Jian. Research on digital image encryption algorithm based on double logistic chaotic map **https://rdcu.be/cZMbG**

[6] Zeng, W., Lei, S.M.: Digital image scrambling for image coding systems. US Patent 6,505,299 (2003)

[7] Wei-Bin, C., Xin, Z.: Image encryption algorithm based on Henon chaotic system. In: 2009 International Conference on Image Analysis and Signal Processing, IEEE, pp. 94–97 (2009)

[8] Chanil Pakbc Lilian Huanga A new color image encryption using combination of the 1D chaotic map - ScienceDirect