AN IMPROVED HYBRID CRYPTOGRAPHIC ALGORITHM USING CHAOTIC MAPS

A. M. S. P. Attanayake, N. Yapage
University of Ruhuna, Matara, Sri Lanka

Chaos theory, chaotic maps, in particular, is playing an increasing role in data encryption and decryption. This research study investigates the application of chaos theory to image encryption and proposes a novel algorithm for image encryption that was derived from two different chaotic maps: Arnold's Cat Map and Bülban Map. In addition to gaining an understanding of the mathematical characteristics, especially the chaotic nature of the two chaotic maps, the objective of the present work is to develop an effective method for encrypting images using the above two chaotic maps. First, the image was encrypted using the two maps individually to analyse their behaviour and encryption patterns and then the maps were combined into a single algorithm. The encryption technique was developed using MATLAB version 2017b. The usefulness of the map was determined by calculating the cross-correlation, vertical, horizontal, and diagonal correlations of the encrypted image, together with its entropy, PSNR (Peak Signal-to-Noise Ratio), and the amount of time that had elapsed before encryption began. In addition, a key sensitivity investigation was carried out to establish the key's level of resistance to force. The fact that the correlation values were substantially closer to zero served as conclusive evidence that the encryption algorithm is successful across all image file types.

The effectiveness of the encryption technique was determined by the entropy levels of the data as well as the PSNR values. In addition, a trial-and-error method was employed to figure out the parameter range in which the Bülban map would display chaotic characteristics.

The proposed algorithm was tested using black-and-white images (512×512 pixels) in the TIFF (257KB), PNG (834KB), and JPEG (111KB) file formats. The ability to encrypt colour images in any format can similarly be developed with this method. Based on the results obtained by encrypting the images using single maps and the hybrid map, it was found that the hybrid map was more efficient. In comparison to utilizing only one of these maps for image encryption, employing both Arnold's Cat Map and Bülban Map with iteration number 170 for Arnold's Cat Map significantly improves the accuracy of the encryption process.

Keywords: Cryptography, Chaotic maps, Image encryption, Arnold’s cat map, Bülban map

AN IMPROVED HYBRID CRYPTOGRAPHIC ALGORITHM USING CHAOTIC MAPS FOR IMAGE ENCRYPTION AND DECRYPTION

A. M. S. P. Attanayake, N. Yapage
University of Ruhuna, Matara, Sri Lanka

INTRODUCTION

Cryptographic systems are utilized to secure the communication links between various devices, and software applications by means of encryption and decryption of multimedia. Modern cryptography utilizes mathematical concepts and algorithms to encode data in a manner that is challenging to decipher. Deterministic algorithms are employed for various purposes such as cryptographic key generation, digital signing, and data privacy verification (Liu et al., 2018). Encryption methods, including DES, AES, and RSA, are not suitable for protecting image data because of the high volume, redundancy, and correlation of visual information (Teh et al., 2020).

The utilization of chaotic maps in encryption is attributed to their properties of randomness, ergodicity, and sensitivity to parameters and initial values. Chaotic maps are a type of dynamical system that exhibits chaos when their parameters are chaotic and are characterized by their iterative nature (Kocarev, 2001). Due to their sensitivity to initial conditions and system configurations, as well as their blending properties, chaotic systems have the potential to be utilized in the design of highly effective cryptosystems (Chaudhary et al., 2022). The process of image encryption involves the use of mathematical algorithms to convert the original image into an incomprehensible form, enhancing its resistance to security breaches such as statistical, differential, and brute force attacks (Li et al., 2018) (Muthu & Murali, 2021). In the past few years, there have been notable advancements in the field of image cryptography algorithms. The utilization of cryptographic algorithms based on chaos has revealed novel approaches toward the creation of image encryption protocols that are highly effective.

METHODOLOGY

The main objective of this work is to encrypt the greyscale image formats tiff (257KB), jpeg (111KB), and png (834KB). The images (512×512 pixels) were retrieved from the image database at https://sipi.usc.edu/database/database.php?volume=misc, a repository that supports image processing research. The tiff images were obtained and converted to jpeg and png formats.

The Bülban map given by $x_{n+1} = x_n \times (a / x_n - b)^{1/2}$ where a and b are real parameters, exhibits the chaotic property known as a sensitive dependency for initial conditions with x values greater than 2 and period-doubling when a is varied and b is set to 2 when bifurcation graph is drawn. As a = 0.5 is approached, the values fluctuate between sixteen and thirty-two distinct values until the system collapses into chaos. If the highest Lyapunov exponent is positive, chaos exists. As shown in Figure 2, the highest Lyapunov exponent for this map occurs at a = 0.5.

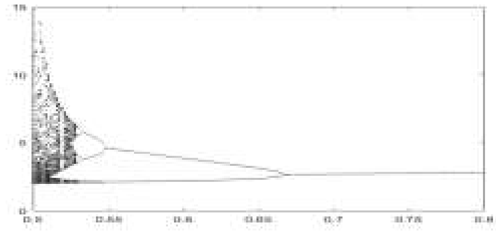

Figure 1 Bifurcation Diagram

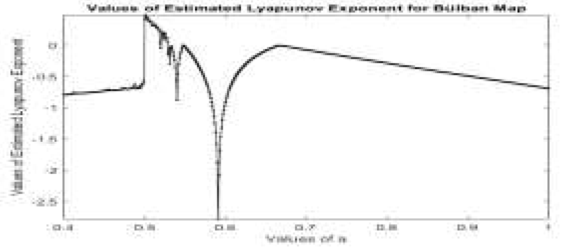

Figure 2 Lyapunov Exponent Graph

In (Alpar, 2014), the map was generalized by selecting $x_0 > b = 4a$. As shown in Figures 3, 4, 5, and 6, the map exhibited chaotic behavior up to b = 3a, 4a, 5a, and 6a when the cobweb plot was generated by modulating the value of b. Nevertheless, not for values greater than that. Three phases were created to clarify the use of individual maps and hybrid map in encryption algorithms. The original image was encrypted using a method that exclusively employs the Bülban map. Given the initial image, the algorithm interprets it as a matrix. The procedure was then reversed to decrypt the cipher image obtained. An algorithm using Arnold's cat map to determine the required number of iterations was then applied to the original image.

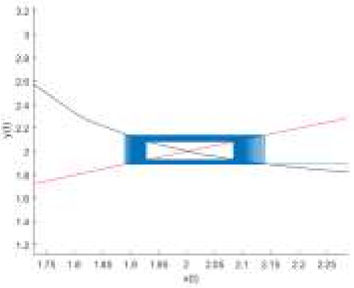

Figure 3 Cobweb Plot b = 3a

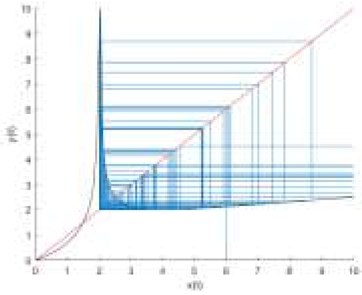

Figure 4 Cobweb Plot b = 4a

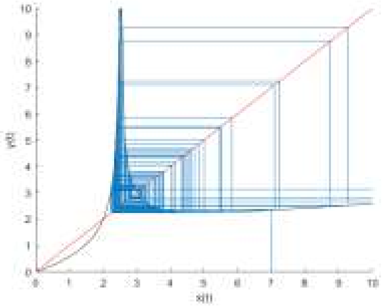

Figure 5 Cobweb Plot b = 5a

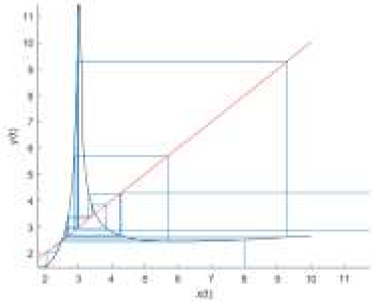

Figure 6 Cobweb Plot b = 6a

After several iterations that is less than the period of the image, all pixels should return to their original positions. Arnold’s cat map is given by *(x, y) → (2x+y, x+y) mod 1*

The process was repeated after determining the number of times the algorithm would be applied to the image. The particles migrate at random across the pixel matrix to encrypt the image. Using the inverse matrix of Arnold’s cat map, the encrypted image was deciphered.

Combining the two preceding encryption algorithms was the final step in developing the proposed algorithm. Using Arnold’s cat map, the original image was muddled, resulting in an indistinct image i_a. It is then fed into an algorithm that uses the Bülban map to produce i_b, the final encrypted image. The final image was constructed using the same technique as the Bülban map. The parameter (p) of the function for a key generation was chosen regardless of image size or type. The user selects p, which expands the encryption key space. According to (Alpar, 2014), the parameter value of 0.5 was chosen for the Bülban map depicting chaotic behavior. The number of iterations for Arnold’s cat map must be less than its period. This parameter increased the cat map's unpredictability.

Following the generation of the cipher image, the suggested map was examined. Tests were conducted to determine the horizontal, vertical, diagonal, and cross-correlation values of neighboring pixels. For each phase, the entropy and PSNR of the original image and the encrypted image were compared, and a histogram analysis was conducted.

RESULTS AND DISCUSSION

Figures 7, 8, and 9 depict the original, encrypted, and decrypted images, respectively. In Figure 7, the encrypted images obtained after 170 iterations displayed patterns, while some iterations yielded indistinct images of the original images. The images in Figures 8 and 9 were, however, more arbitrary due to the diffusion of the pixels.

Original image correlation values were closer to 1, indicating significant positive correlations between horizontal, vertical, and diagonal pixels. Except when only Arnold’s cat map technique was used, all correlation values were closer to 0 up to two decimal places after encryption, except when only Arnold’s cat map technique was used. This illustrates the substantial difference between encrypted and original images. The entropy of the original image and the image encrypted using Arnold’s cat map alone was identical. By utilizing both maps, the entropy of the encrypted images has been increased. With more noise added to an image, the PSNR decreased as it becomes less meaningful.

When both maps were utilized, the PSNR value decreased, as the encryption phase introduced more noise.

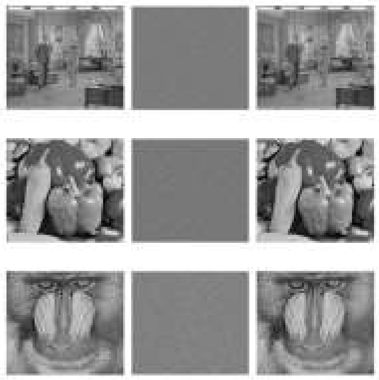

Figure 7 Encryption and Decryption Results Using Arnold's Cat Map

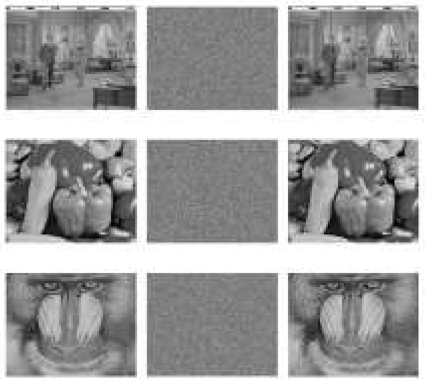

Figure 8 Encryption and Decryption Results Using Bülban Map

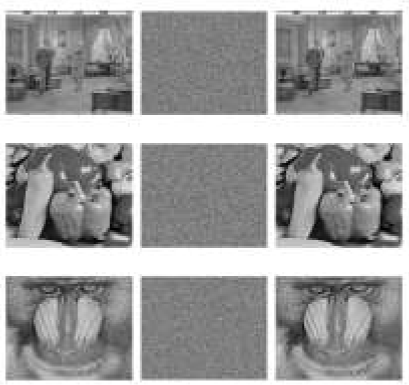

Figure 9 Encryption and Decryption Results Using Hybrid Map

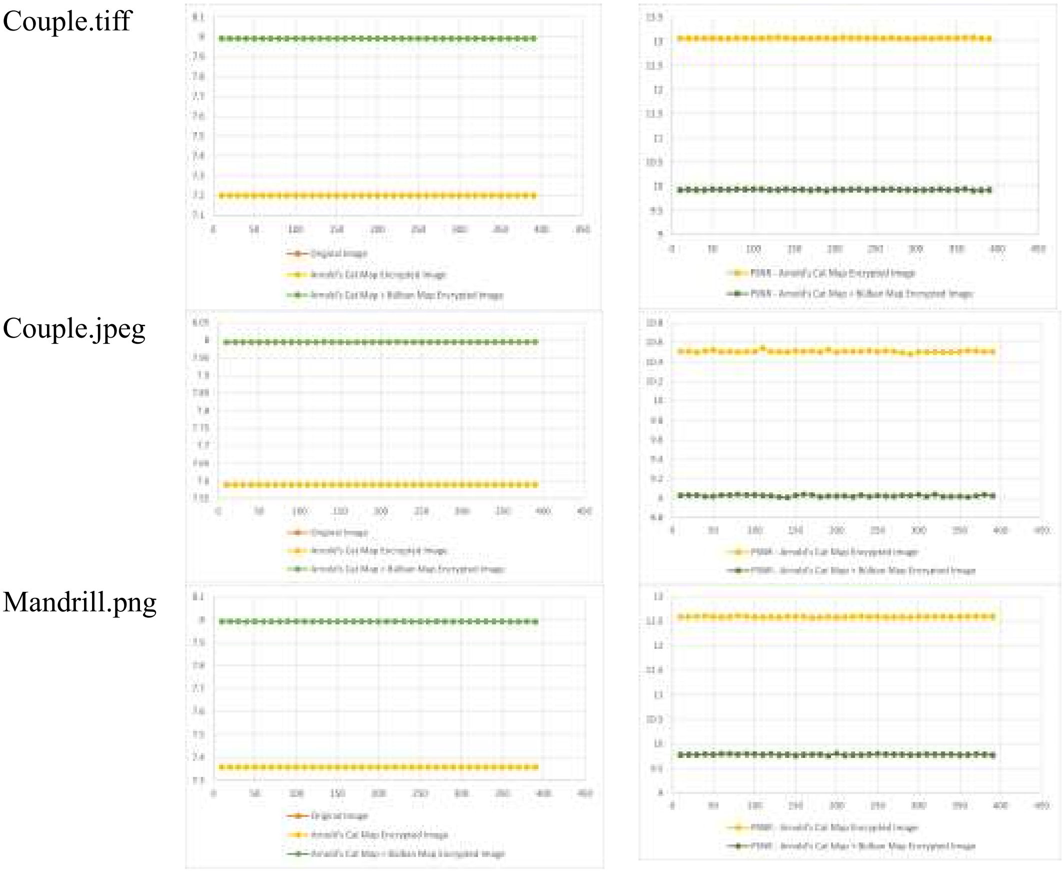

Figure 10 Entropy and PSNR Values for Images Respectively

Arnold’s cat map did not add noise or additional information to the pixels, whereas the Bülban map in figures 8 and 9 did, resulting in pixels that were randomized. This is because the PSNR and entropy values of the encrypted Arnold’s cat map images are identical to the values of the original images. Arnold’s cat map is simple and effective at combining image pixels and removing their correlation, but it is insensitive to changes in its governing parameters. Using Arnold’s cat map to jumble an image, the image can be reassembled by repeatedly iterating the chaotic map and modifying its parameters. We can therefore affirm that this encryption method does not add any additional data to the images. When the Bülban map was utilized, however, additional information was added to the pixels of the original image based on the map's encryption key, resulting in differentially ascribed pixels, which led to decreased correlation values, increased entropy, and decreased PSNR values.

CONCLUSIONS / RECOMMENDATIONS

Based on the findings, it can be concluded that the composite map exhibited greater efficacy compared to either of the individual maps. Upon conducting individual analyses of each map, it was observed that the Bülban map exhibited superior performance. This can be attributed to the fact that the Bülban map incorporated additional information into the pixels by changing their values, rendering them more randomized in appearance. Arnold's cat map was found to be inadequate in generating the necessary entropy for the encryption, resulting in a reduction of its resistance against brute-force attacks. Each of the three algorithms has the potential to be utilized for encryption purposes, however, hybrid encryption is deemed to provide the utmost level of security based on the results and the conclusions made (Dureja & Kochhar, 2015).

The study employed grayscale photographs in the formats of tiff, png, and jpeg to evaluate the efficacy of the encryption system. This study exhibits potential for further expansion, wherein the identical approach can be applied to encrypt color images of diverse formats.

Subsequent to the current stage of the investigation, it may be prudent to explore higher-dimensional chaotic map methodologies, specifically those of 3d and 4d, in order to construct a robust and efficacious image encryption infrastructure (Zia et al., 2022). Subsequently, cryptanalysis may be carried out on the assessed algorithms to ascertain their potential vulnerabilities and strengths against attacks.

REFERENCES

Alpar, O. (2014). Analysis of a new simple one dimensional chaotic map. *Nonlinear Dynamics*, *78*(2), 771–778. https://doi.org/10.1007/s11071-014-1475-1

Chaudhary, N., Shahi, T. B., & Neupane, A. (2022). Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. *Journal of Imaging*, *8*(6). https://doi.org/10.3390/jimaging8060167

Dureja, P., & Kochhar, B. (2015). *Image Encryption Using Arn old ' s Cat M ap and Logistic Map for Secure Transmission*. *4*(6), 194–199.

Kocarev, L. (2001). Chaos-based cryptography: A brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6–21. https://doi.org/10.1109/7384.963463

Li, X.-Z., Chen, W.-W., & Wang, Y.-Q. (2018). Quantum Image Compression-Encryption Scheme Based on Quantum Discrete Cosine Transform. *International Journal of Theoretical Physics*, *57*, 1–16. https://doi.org/10.1007/s10773-018-3810-7

Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., & Miao, S. (2018). Image block encryption algorithm based on chaotic maps. *IET Signal Processing*, *12*(1), 22–30. https://doi.org/https://doi.org/10.1049/iet-spr.2016.0584

Muthu, J. S., & Murali, P. (2021). Review of Chaos Detection Techniques Performed on Chaotic Maps and Systems in Image Encryption. *SN Computer Science*, *2*(5). https://doi.org/10.1007/s42979-021-00778-3

Teh, J. Sen, Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, *50*(November). https://doi.org/10.1016/j.jisa.2019.102421

Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *International Journal of Information Security*, *21*(4), 917–935. https://doi.org/10.1007/s10207-022-00588-5