An Investigation into the Usage of Bounding Boxes in Discriminating Image Encryption Algorithms

Geetanjli Khambra, Vijay Panse and Shilpa Jackson
Department of Computer Applications, The Bhopal School of Social Sciences, Bhopal, India

Keywords: Bounded Box, Image Encryption, Decryption, Correlation.

Abstract: When it comes to protecting people's privacy and maintaining secrecy, encrypting photographs is the safest and most effective method. However, the computational expense and treating time required to conduct complete image encryption prove to be preventive constraints that preclude it from presence employed more intensively in real time. This is because of the large size and complicated nature of digital images. In order to solve this issue, many recent studies have turned to selective encryption, a way of encrypting only the most salient features of an image in an effort to lessen the encryption burden. As a possible contribution, we offer a selective picture encryption method that uses bounded boxes. The computational repercussions of selective image encryption have been the subject of experimental studies. It has been determined through testing that the selective encryption technique is significantly faster than other methods of encryption. Selective encryption has these features; hence it can be looked at as a viable option. Therefore, this contribution improves security to an acceptable level during implementation. Experiments with the same have shown promising results in protecting real-time photos.

1 INTRODUCTION

The best way to ensure privacy and maintain confidentiality with photographs is to encrypt them. However, the calculation expense and treating time required to conduct complete image encryption prove to be preventive constraints that preclude it from presence employed more intensively in real time (Dworak et al., 2016). This is because of the large size and complicated nature of digital images. In order to solve this issue, many recent studies have turned to selective encryption, a way of encrypting only the most salient features of an image in an effort to lessen the encryption burden. However, a fair comparison of its performance to full encryption is needed (Enayatifara et al., 2017; Yavuz and Yazici, 2016; Faragallah, 2013).

The most widely used framework for encrypting images in a chaotic environment is based on a special set of rules for selective picture encryption (Fister and Tepeh (2016). The effect of a single pixel can be correctly diffused to the whole cipher-photo with numerous conventional rounds of encryption using the substitution method, in which the pixel values are modified sequentially, with the alteration completed to a precise pixel usually depending on the collected impact of all the preceding pixel values (Wang et al., 2016; Gu and Ling, 2014; Chen et al., 2017; Chen et al. 2015). To generate a pseudorandom key stream for replacement, one can use a logistic map, tent map, or Lorenz machine, to name just a few of the many discrete and continuous chaotic structures available (Shi et al. 2016). The secret password is featured in the hired chaotic systems' starting parameters and conditions.

The phases of permutation and substitution are typically considered neutral. Because the permutation method best reshuffles the pixel placements while without pixel price, it is vulnerable in the course of some of the commonplace attacks, specifically statistical assaults and seemed/chosen simple text attacks (Jolfaei and Mirghdri, 2011; Lang, 2015; Wang et al. 2015; Li, 2016). Pixel charge permutation and substitution (PS/2) plain-photo Cipher-photo iterations rounds Using the Permutation Key Chaos-based image cipher substitution key common form. The replacement method is secure, but it is computationally intensive. The permutation method is much simpler (Su and Gao, 2013).

This is owing to the fact that computations are carried out over the field of actual numbers, and a fantastic widespread variety of iterations of a chaotic

Khambra, G., Panse, V. and Jackson, S.
An Investigation into the Usage of Bounding Boxes in Discriminating Image Encryption Algorithms.
DOI: 10.5220/0012491600003739

In *Proceedings of the 1st International Conference on Artificial Intelligence for Internet of Things: Accelerating Innovation in Industry and Consumer Electronics (AI4IoT 2023)*, pages 397-402
ISBN: 978-989-758-661-3

map is required for the vital thing movement creation technique (Sui and Lu, 2014). The computational precision cannot be a factor in a key sensitivity analysis of a crypto-instrument. This work introduces a hybrid model based replacement technique to enhance the performance of the chaos-based selective picture cryptosystem (Sui et al., 2015).

The advantages of the digital revolution haven't been realized without costs, such as restrictions on copying and sharing digital multimedia system papers. In order to rise to this challenge, academics have been working tirelessly to develop novel and cost-effective document protection strategies for use in multimedia system documentation. In this setting, new methods such as coded writing and digital watermarking are introduced (Wang et al., 2015) . Another method of protecting the ownership and authenticity of digital multimedia system material consists of adding digital watermarks to relevant documents. As the Internet expands and transmission technology becomes more commonplace, people will find it easier than ever to share digital transmission data like digital images with one another online (Wangm and Zhang, 2016).

The purpose of this study is to develop a more secure image encryption technique based on dispersal and misperception. Image encryption utilizing the diffusion and confusion techniques, image encryption using genetic operators, and selective image encryption using chaos on a Windows machine are all within the scope of this article.

2 EXISTING WORK DONE

By combining a logistic map with a cellular automaton, the authors have provided a method for computing picture encryption. The plan combines two different types of randomizations, permutation and diffusion (Liu and Sun, 2016). The pixels are shuffled using a permutation technique, and then the dispersion system amplifies the effects of even a single pixel's alteration throughout the entire image. The calculation is based on a muddled system, so even a minor shift in the significant will harvest drastically different results. The suggested framework's key feature is its ability to limit attacks using animal power and to function in noiseless transmission. The article also suggests that the framework has strong security based on the results of key sensitivity analysis, histogram analysis, differential attack, and other testing (Wu et al., 2015).

This academic study details a quick method of image encryption. Here, a 2D Sine IMIC Modulation map is used, and its unstructured capabilities are analysed using a stage chart, a Lyapunov type range, and a many-sided quality. At the foundational stage of encryption, the confusion and dissemination method are consolidated. The pixels in the image can be jumbled up very efficiently using a technique called Chaotic Shift Transform (CST). In addition, a method of line and segment replacement is used to reorder the pixels in the image. The scrambling effect and low-time many-sided quality of CST are superior. In this instance, we employ the utilization of several different keys. A 256-bit secret key is sufficient to withstand a brute-force attack (Zhang et al. 2013).

Researchers presented an encryption scheme based on connecting various chaotic maps to provide secure transmission of therapeutic images. Logistic, tent, and sine maps are all incorporated into the suggested procedure. In this method, DICOM picture pixels are muddled and spread out (Zhang et al. 2012). The manufactured chaos-cryptic arrangement is submitted to a number of security investigations, including measurable, differential, key space, key affectability, deliberate scrambling assault, and select plaintext attack tests, to validate the severity of the proposed approach. Measurement analysis, connection analysis, differential analysis, key space analysis, key affectability analysis, deliberate trimming attack analysis, and picked plaintext attack analysis are just some of the systems used in this paper to analyse and approve the security and unpredictability of the proposed plan (Zhang et al. 2014).

In order to optimize for the monarch butterfly, the authors advocated a greedy approach combined with a self-adaptive crossover operator (GCMBO). Movement Administrator and Butterfly Changing Administrator are combined into one eager system in GCMBO. Better performance is possible in the future if more benchmark issues are used, especially real-world applications (Liu and Li, 2013). Using LTSVR (Lagrangian twin support vector relapse) and HC (hereditary calculation) in DCT (discrete Cosine transform) space, researchers offer a safe and robust grey scale picture watermarking scheme (Hua and Zhou, 2016). The key components into which the watermark will be embedded are determined using fuzzy entropy. The inability to withstand rotational and translational attacks is a major shortcoming. Under the available computational asset, authors offer an autonomous multi-objective advancement model that can account for security and quality of service (Wang et al., 2019).

3 THE PROPOSED WORK

This work introduces a hybrid model based replacement technique to enhance the performance of the chaos-based selective picture cryptosystem. The following details the suggested architecture for a replacement method for selective picture encryption with a key generated via chaos-based key generation.

1.1. The face detector is used to identify the one-of-a-kind photo. The resulting binary image will be the same size as the original photograph but will only include the numbers 1 and 0. A value of one indicates that the area is in the same location as the corresponding pixel in the original image, whereas a value of zero indicates that there is no area there.

1.2. The original imagery is converted to a series of zeros and ones, known as binary. The special photographic archive will be discarded. Subtracting anything from the past (foreground detection) is another name for this technique.

1.3. The goal of selective encryption is to reduce the number of photos that need to be encrypted without compromising security. Selective encryption methods require the original image to be chosen.

1.4. To substitute means to change the location of a pixel in a picture from one location to another. In this process, the partial encrypted image is encrypted using a substitution method based on Hybrid T models.

Algorithm for the proposed method is as follows:

1. Twitch with your original coloured medicinal image.
2. Grayscale and binary formats can be created from the provided image.
3. The multi-chaotic key is used for selective encryption, which results in the scrambled images.
4. Images with selective encryption using the S-Box produce encrypted versions of themselves.

The Inverse hybrid substitution method, which makes use of both key stream and Inverse image conversion techniques, is the foundation of secure and selective Chaos-based image encryption (SSIE). Figure 2 displays a square chart of the suggested unscrambling algorithm.

Combining key stream and Inverse image conversion methods, a decrypted picture can be derived from the encrypted image using the Inverse hybrid substitution process.

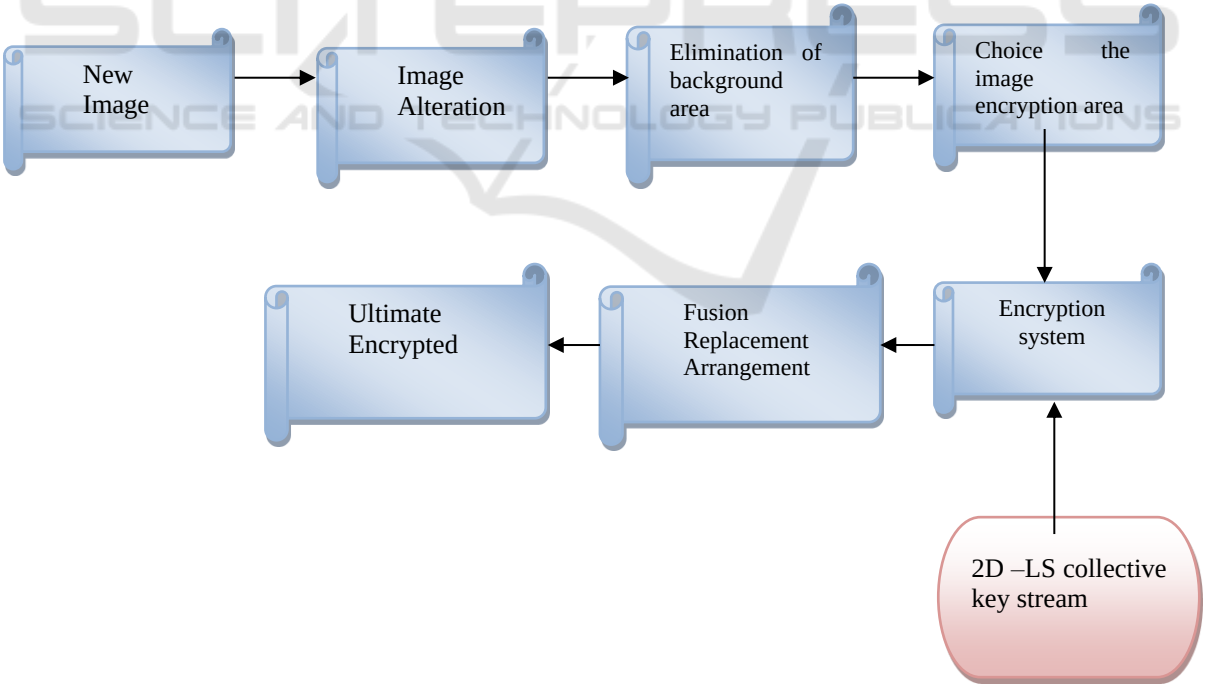

Figure 1: The Proposed Block Diagram.

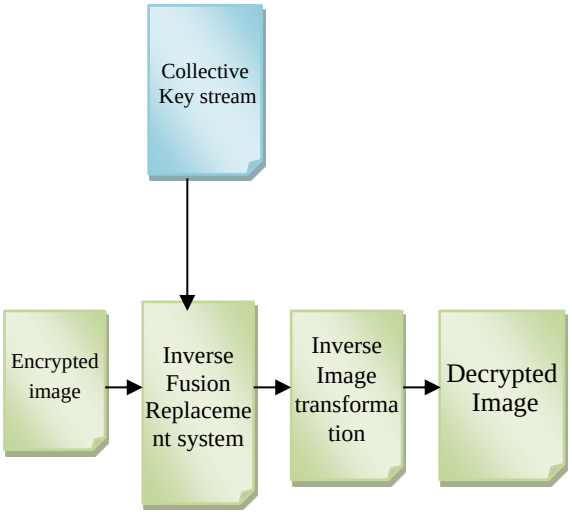

Figure 2: Square Chart of SSIE Decryption Process.

4 RESULT ANALYSIS AND DISCUSSION

This experiment is performed using MATLAB R2010a, with key generation based on randomness. Here, authors have discussed about the connection coefficients, key space inquiry, key affectability research, and differential investigation that were run on the proposed plot.

1.5. Association analysis: The first image's neighbouring pixels are very closely related along the horizontal, vertical, and oblique axes. Pixels in the encrypted image should have relationship coefficients that are sufficiently small to withstand quantifiable attacks if the encryption computation was performed correctly.

$$Corr\left(\frac{A}{B}\right) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{i,j}-\hat{A};\ B_{i,j}-\hat{B})}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(A_{i,j}-\hat{A})^2\ \sum_{i=1}^{m}\sum_{j=1}^{n}(B_{i,j}-\hat{B})^2}} \quad (1)$$

A random comparison of 2000 pairs of nearby pixels in each direction is made with the encoded equivalents of the images. This is done so that the associations between close pixels in the plain and figure images can be analysed and thought about. Figure 3 presents the correlation coefficient for both the unencrypted and encrypted versions of the image. Images that have been encrypted have a more consistent grayscale than their plain counterparts.

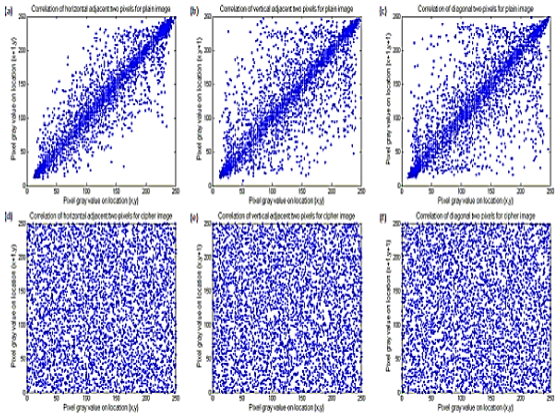

Figure 3: Association of Input Images and the analogous Ciphered Images.

1.6. Information Entropy Analysis: In order to objectively assess risks, one can use data entropy. The information entropy of a figure picture is calculated in order to evaluate his eccentric behaviour. The maximum entropy for a grayscale image is log (28) = 8 and will be attained if the pixels appear with equal probability, as there are 28 possible grayscale quality.

1.7. We use two quantitative metrics—the Number of Pixel Change Rate and the United Average Changing Intensity—to examine the effect of a single pixel change in the plain-image on the cipher-image, ensuring the proposed encryption system is resistant to differential attack.

$$NPCR = \frac{1}{MxN} * \sum_{i,j} D(i,j) * 100\% \quad (2)$$

Any modification to the plaintext picture must result in a corresponding modification to the cipher text image. The average pixel-wise intensity difference between the two images can be determined with the aid of UACI. Images 'C1' and 'C2' are of the same size.

$$UACI = \frac{1}{MxN} * \sum_{i,j} [\frac{C1(i,j) - C2(i,j)}{225}] * 100\% \quad (3)$$

Table 1: Different evaluation parameter comparison.

S. No.	data	Evaluation parameters		
		Entropy	NPCR	UACI
1	Lungs	7.97	99.76	33.34
2	Eye	7.96	99.45	33.57
3	Heart	7.95	99.32	33.61
4	Bone	7.96	99.84	33.71

The entropy of several example photos is displayed in Figure 4. The ability of the suggested cryptosystem to withstand entropy attacks has been widely established. The lungs are the most entropic organ in the body. This can be checked by comparing the cypher images derived from a standard photo to one derived from a picture with a single altered pixel. Adjusted pixel count is the foundation of NPCR. The NPCR value of several test photos is displayed in Figure 4. Here, the NPCR and UACI values in bone are the highest.

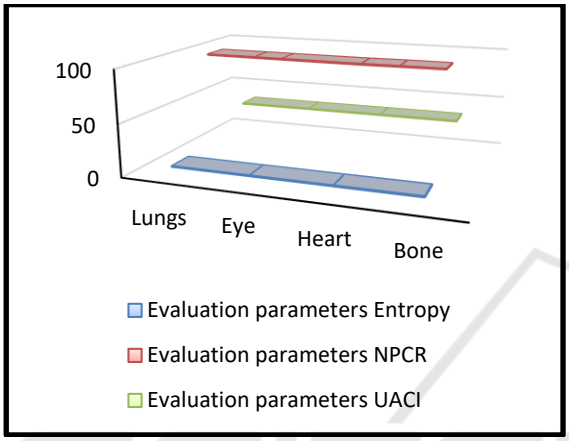

Figure 4: Different evaluation parameter comparison.

5 CONCLUSION

Substitution systems were used in the selective image encryption. The majority of critiques in this field rely on confusing pixel-based substitution schemes and other forms of random substitution. While effective, such encryption methods are unlikely to provide as much protection as do conventional numbers, which are less vulnerable to attacks. Therefore, specific encryption of restorative images based on substitution computation is a better trade-off between security and efficiency.

This work presents a hybrid confusion-based strategy for selective picture encryption that makes use of bounded boxes. There was a significant decrease in required processing time and a noticeable improvement in security. The proposed approach promises a universally applicable selective encryption algorithm that may be implemented across a wide variety of computer distributed systems for safe, scalable cloud data storage.

REFERENCES

Dworak, K, Nalepa, J, Boryczka, U & Kawulok, M (2016), 'Cryptanalysis of SDES using genetic and memetic algorithms', Springer Computational Intelligence, vol. 642, no. 18, pp. 3-14.

Enayatifara, R, Abdullahb, AH, Isninb, IF, Altameemc, A & Leed, M (2017), 'Image encryption using a synchronous permutation-diffusion technique', Optics and Laser in Engineering, vol. 90, no. 2, pp. 146-154.

Erdem Yavuz & Rifat Yazici (2016), 'A chaos-based image encryption algorithm with simple logical functions', Computers and Electrical Engineering, vol. 54, no. 1, pp. 471 - 483.

Faragallah, OS (2013), 'Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain', International Journal of Electronics and Communication, vol. 67, no. 3, pp. 189-196.

Fister, I & Tepeh (2016), 'Epistatic arithmetic crossover based on Cartesian graph product in ensemble differential evolution', Applied Mathematics Computation, vol. 283, no. 18, pp. 181-194.

Gai-Ge Wang, Suash Deb & Xinchao Zhao (2016), 'A new monarch butterfly optimization with an improved crossover operator', Springer, vol. 18, no. 3, pp. 731-755.

Guosheng Gu & Jie Ling (2014), 'A fast image encryption method by using chaotic 3D cat maps', Elsevier-Optik, vol. 125, no. 17, pp. 4700-4705.

Hang Chen, Camel Tanougast, Zhengjun Liu & Loic Sieler (2017), 'Asymmetric optical cryptosystem for color image based equal modulus decomposition in gyrator transform domains', Optics and Laser Engineering, vol. 93, no. 1, pp. 1-8.

Hang Chen, Jiguang Zhao, Zhengjun Liu & Xiaoping Du (2015), 'Optodigital spectrum encryption by using Baker mapping and gyrator transform', Optics and Lasers in Engineering, vol. 66, no. 1, pp. 285-293.

Jinhua Shi, Hui Lu & Kefei Mao (2016), 'Solving the Test Task Scheduling Problem with a Genetic Algorithm Based on the Scheme Choice Rule', Springer, vol. 9713, no. 1, pp. 19-27.

Jolfaei, A & Mirghdri, A (2011), 'Image encryption using chaos and block cipher', Computer and Information Science', vol. 4, no. 1, pp. 172-185.

Jun Lang (2015), 'Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain', Optics Communications, vol. 338, no. 1, pp. 181-192.

Kai Wang, WJ, Pei, LH, Zou, Aiguo Song & Zhenya He (2015), 'On the security of 3D Cat map based symmetric image encryption scheme', Physics Letter A, vol. 343, no. 6, pp. 432-439.

Li, C (2016), 'Cracking a hierarchical chaotic image encryption algorithm based on permutation', Signal Processing, vol. 118, no. 2, pp. 203-210.

Liansheng Su & Bo Gao (2013), 'Single-channel color image encryption based on iterative fractional Fourier

transform and chaos', Optics & Laser Technology, vol. 48, no. 1, pp. 117-127.
Liansheng Sui & Haiwei Lu (2014), 'Double-image encryption using discrete fractional random transform and logistic maps', Optics and Lasers in Engineering, vol. 56, no. 1, pp. 1-12.
Liansheng Sui, Kuaikuai Duan & Junli Liang (2015), 'Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps', Optics Communications, vol. 343, no. 1, pp. 140-149.
Wang, XY, Zhang, YQ & Bao, XM (2015), 'A novel chaotic image encryption scheme using DNA sequence operations', Optics and Lasers in Engineering, vol. 73, no. 1, pp. 53-61.
Wangm, X & Zhang H (2016), 'A novel image encryption algorithm based on genetic recombination and hyper chaotic systems', Nonlinear Dynamics, vol. 83, no. 2, pp. 333–346.
Wenhao Liu & Kehui Sun (2016), 'A fast image encryption algorithm based on chaotic map', Optics and Lasers in Engineering, vol. 84, no. 1, pp. 26 - 36.
Wu, X, Kan, H & Kurths, J (2015), 'A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps', Applied Soft Computing, vol. 37, no. 1, pp. 24-39.
Zhang, Q, Guo, L & Wei X (2013), 'A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system', Optik - International Journal for Light and Electron Optics, vol. 124, no. 18, pp. 3596-3600.
Zhang, Y, Li, C, Li, Q, Zhang, D & Shu, S (2012), 'Breaking a chaotic image encryption algorithm based on perceptron model', Nonlinear Dynamics, vol. 69, no. 3, pp. 1091-1096.
Zhang, Y, Wen, W, Su, M & Li, M (2014), 'Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system', Optik - International Journal for Light and Electron Optics, vol. 125, no. 4, pp. 1562-1564.
Zhengjun Liu & She Li (2013), 'Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding', Optics and Lasers in Engineering, vol. 51, no.1, pp. 8-14.
Zhongyun Hua & Yicong Zhou (2016), 'Image encryption using 2D Logistic-adjusted-Sine map', Information Sciences, vol. 339, no. 20, pp. 237 - 253.
Wang, C.P.; Wang, X.Y.; Xia, Z.Q.; Zhang, C., (2019), 'Ternary radial harmonic Fourier moments based robust stereo image zero water marking algorithm'. Inf. Sci. 2019, 470, 109–120.