An Improved Analysis of Secured Permutation and Substitution based Image Encryption

Vikas Goel[1], Amit Kumar Goyal[2]

[1]Department of Information Technology, Kiet group of institutions, Ghaziabad, India

[2] Department of CA, Kiet group of institutions, Ghaziabad, India

Emails: vikas.goel@kiet.edu; Amit.goyal@kiet.edu

Abstract

The transmission and storage of digital data raises serious security concerns as information technology evolves at a breakneck pace. To ensure the safety of the transferred data, security methods must be put in place. Encrypting an image is a method of protecting sensitive data by converting it into an unrecognizable format. The procedure includes access control, privacy, validation, and copyright protection. Cryptography, steganography, and watermarking are three distinct methods to prevent unauthorized access to digital data. Of these three methods, cryptography has emerged as one of the most important ways to ensure complete safety. Therefore, a secure and efficient cipher algorithm is required for trustworthy communication. In this work, we offer a practical Secured Asymmetric Image Cipher (SAIC) Algorithm for encrypting images with a secret key of arbitrary length. At first, the KG algorithm creates two unique keys. Both the encryption and decryption processes require a key. The experimental results reveal that the encrypted image lacks the original image's independence (NPCR > 99.89%, UACI > 36.89%). The suggested approach has a high encryption rate, can be implemented easily, and is computationally secure. The reproduced data validates the safety and practicability of the proposed architecture.

Keywords: Image Encryption; SAIC; Permutation; Substitution; Secured Asymmetric Image Cipher

1. Introduction:

Information security, or cryptography, is the study of methods to transmit data securely between end users while keeping that data private. When the demand for secrecy was at its highest, like during globe War II, the globe saw the development of effective encryption methods. This marked the beginning of the age of information technology. Since most information is transmitted through a public channel that is prone to security breaches, protecting it is essential [1]. Images are efficient candidates for information conveyance because they condense potentially confusing nuance into a small number of pixels. Images have become an integral part of many organizations, from government hubs to panchayat hospitals in sleepy rural communities. This justifies the urgent requirement for a reliable and secure image encryption technology [2].

Mapping data from one domain to another within the same domain is essential to every cryptosystem. Encryption refers to a specific mapping algorithm, and decryption describes the inverse of that process [3-4]. The mathematical structure of the message will be preserved in the encrypted symbols. Symbols have to be part of a finite group, ring, or field since their number is finite. Algebraic manipulations are applied to the symbols of a finite group, ring, or field in order to use them as ciphers. Algebraic cryptosystem is another name for it because of this. In particular, the linear algebraic principle is applicable across the finite field, ring, or group [5-6].

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

There are two main types of cryptography: symmetric and asymmetric keys. The private-key encryption algorithm used in symmetric cryptography provides both the sender and the recipient with the same secret key. Given the lack of privacy between the sender and the receiver in the cryptosystem, the decryption key is simply the inverse of the encryption key and can be easily formulated. In contrast, two keys are required for asymmetric cryptography [7]. There are two types of encryption keys: the public-key, which can be shared with anyone, and the private-key, which is known only to the receiver and is used to decrypt communications and verify signatures. It's not easy to get a hold of the private key because it relies on secret parameters that only the receiver knows. One essential security method is encryption, or the scrambling of data. When used correctly, it can provide a safe means of communication regardless of the safety of the underlying system and network [8]. When data travels through shared systems or network segments that are easily accessible to all users, this becomes very crucial. This necessitates the use of encryption to safeguard private information, particularly passwords, from prying eyes outside. Encryption is the process of transforming plaintext into cipher text using a computational process and a key, which is just a huge number coupled with a password or pass phrase. The resultant encrypted message can only be read by the person in possession of the matching key [9]. The process of decoding that occurs on the receiving end is known as decryption. Information security services are essential to the operation of nearly every modern institution, from e-government to financial dealings. Users of these services should be certain of their privacy, their data's integrity, their availability, their invulnerability to forgery, and their authenticity. Privacy is protected through the use of encryption. Message authentication codes, digital signatures, and biometrics are the most common methods for ensuring message authenticity and confidentiality [10]. When taking a broader perspective, network security is also a crucial part of the security service. The application layer, the transport layer, and the network layer are all protected [11].

2. Related Work

An integrated encryption and watermarking system is developed, which uses the quantization record regulation and a cipher computation to replace the need for separate ones. The suggested structure is consistent with the DICOM standard because it uses the Advance Encryption Standard in cipher block chaining mode [12]. Therefore, this approach achieves a very high level of safety.

Here, we use key space analysis, factual investigation, and key affectability to ensure the safety of the new picture encryption computation [13]. Selective image encryption techniques are utilized to facilitate quicker encryption/decryption operation execution. Interest in the co-configuration of hardware and software is on the rise at the present time [14].

It is proposed to use a picture scrambling encryption technique. This method makes it more difficult for an unauthorized person to decipher the encryption. In order to transfer colour images safely over a wireless media, a number of cipher algorithms have been suggested [15]. There are three distinct categories that can be used to categorize these cipher algorithms: diffusion, confusion transformation, and a hybrid of the two. Only a few number of encryption methods have been developed so far that use digital grey pictures as their basis. Original photos should be kept very secret, as their disclosure might cause shame and embarrassment. This means that the storage and transfer of this information must be secure [16].

The resulting result is supposed to make computations more efficient. In these contexts, the genetic algorithm is typically implemented through heuristic enhancement techniques. The information-hiding capability of a genetic-algorithm-based chaotic map is improved [17]. Using a variety of chaotic maps helps increase arbitrary nature. As the fitness function, we choose the Peak Signal-to-Noise Ratio (PSNR). The supplied technique's success lies in the fact that gauss, logistic, and tent maps are much faster than the proposed information hiding technique's arbitrary capacity [18].

The authors created logistic adjusted sine maps that are two-dimensional in their format. It is planned to strengthen the criteria for dispersal and chaos by introducing random components in otherwise straightforward pictures in order to make graphical representations safer. This will be done in order to achieve this goal [19]. It outperforms many existing chaotic maps in terms of ergodicity and flintiness and has a more diffuse confused extent. To increase security and defend against the savage power assault, keys are produced using an asymmetric encryption method with a key space larger than 2100. Set the puzzle key to 232 bits to meet this need and adapt to the LAS-IES architecture [20]. Therefore, LAS-IES can be integrated with automated images from any company. Pixels, bit control complexity, and bit control distribution are all covered across its three parts of guidance. For each mashup to be easily distinguishable, the nearby pixels must contribute arbitrary characteristics to the base image [21]. To satisfy the rule of disarray and distribution, multiple rounds of

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

confusion and spread are done at the bit level. The results of the generation and the analysis of the security demonstrated that LAS-IES can transform any image into an irregular like ciphered image with a high level of security [22].

The study team referred to an adjusted standard guide and a chaos-based picture encryption arrangement. There are two phases to this setup: the first, when the pixel stage and component s-box substitution rearrange the photo and adjust the pixel values, and the second, where the spread is completed in an ad hoc fashion [23]. Using the revised reference, a chaotic key sequence is generated. It is suggested that the layout is depending on the disorganized clustering. For simulation purposes, MATLAB is used to implement the method. Possible phases are numbered from 1 to 16, and among them, only 16 unique variations in the s-box lines are determined [29]. The modified standard guide and element s-box substitution makes the arrangement robust and secure against quantifiable and differential attack, as shown by an analysis using entropy, histogram and connection, NPCR, and UACI values [24].

An epistatic number-crunching hybrid is used in differential development, and the authors' studies on the impact of epistatic qualities in transformative calculation are considered. Each epistatic quality in posterity depends on the comparing hypostatic qualities of its folks. Hybrid in the EA meaning refers to a solution space in which parameters from one guardian are swapped for parameters from the other guardian at the same time, while the hybrid in DE specifies how many parameters should be swapped [25-27]. The group differential development is linked to the epistatic number juggling hybrid as a process of transformation. As a result, epistatic attributes are governed by the straight-line Cartesian graph representation of the results from both guardians. We were inspired to begin experimenting with other diagram objects after seeing excellent results from extensive tests conducted on the CEC-14 capacity benchmark suite.

Scientists have been studying the flight patterns of natural monarch butterflies with the goal of recreating same patterns in the lab. Benchmark evaluation on many unimodal and multimodal test capabilities, compared to five state-of-the-art metaheuristic computations, confirmed MBO's viability. The aforementioned ideology is essentially a variation on the original MBO, enhanced by the Greedy system and the self-versatile Crossover administrator (GCMBO) [28]. During the later run phase of the hunt, the SAC administrator can greatly improve the population's diverse traits by using GCMBO. In butterfly modifying administrator, the greedy approach is used to pick out only the ruler butterfly individuals who are physically fitter and can speed up the assembly process. Finally, 25 industry-standard unimodal and multimodal test capacity are used to compare the provided GCMBO method to the rest of the field. The results reveal that GCMBO can be used to produce results that are vastly superior to those obtained using the standard MBO method [29].

This first edition features the authors' work on a novel impalpable, safe, and robust grayscale picture watermarking strategy based on Discrete Cosine Transform, LTSVR, and genetic calculation. The appropriate squares for watermark installation are selected using fuzzy entropy. The dimensionality of the watermarking problem is reduced and repeated or irrelevant parts are removed when the number of squares is determined based on fluffy entropy. In order to help LTSVR find the non-linear relapse capacity between the information and goal vector, the image dataset is shaped using notable DCT coefficients with high vitality compaction quality of each chosen square. The GA process considers globally defined health capacities to determine the unique watermark quality for each selected square [30]. The watermark is successfully removed from the watermarked images in opposition to a series of image processing operations thanks to the high speculative property of LTSVR and the good learning capacity of picture characteristics.

3. The Proposed Secure Image Encryption Method

Mixing, diffusion, and confusion are the three main components of the Secured Asymmetric Image Cipher (SAIC) system. The proposed encryption and decryption algorithm is shown here. The SAIC encryption calculation square chart is shown in Figure 1. This approach relies on a secret key whose size can change over time. Elements of the original image are degraded throughout the blending process. The resulting encoded picture is cut into several key ward square parts that do not overlap. Dissemination and substitution strategies have set up every square. Diffusion involves rearranging the position of each square's pixels within the puzzle using a multi-stage saw-tooth SFC method. Every pixel in a chaotic image has its attributes altered by the pixels around it. To be more precise, during the distribution process, neighbouring pixels are dispersed uniformly within the image. Both the dispersal and the disarray processes are carried out in secret. The final result of the chaos phase is a totally jumbled image.

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

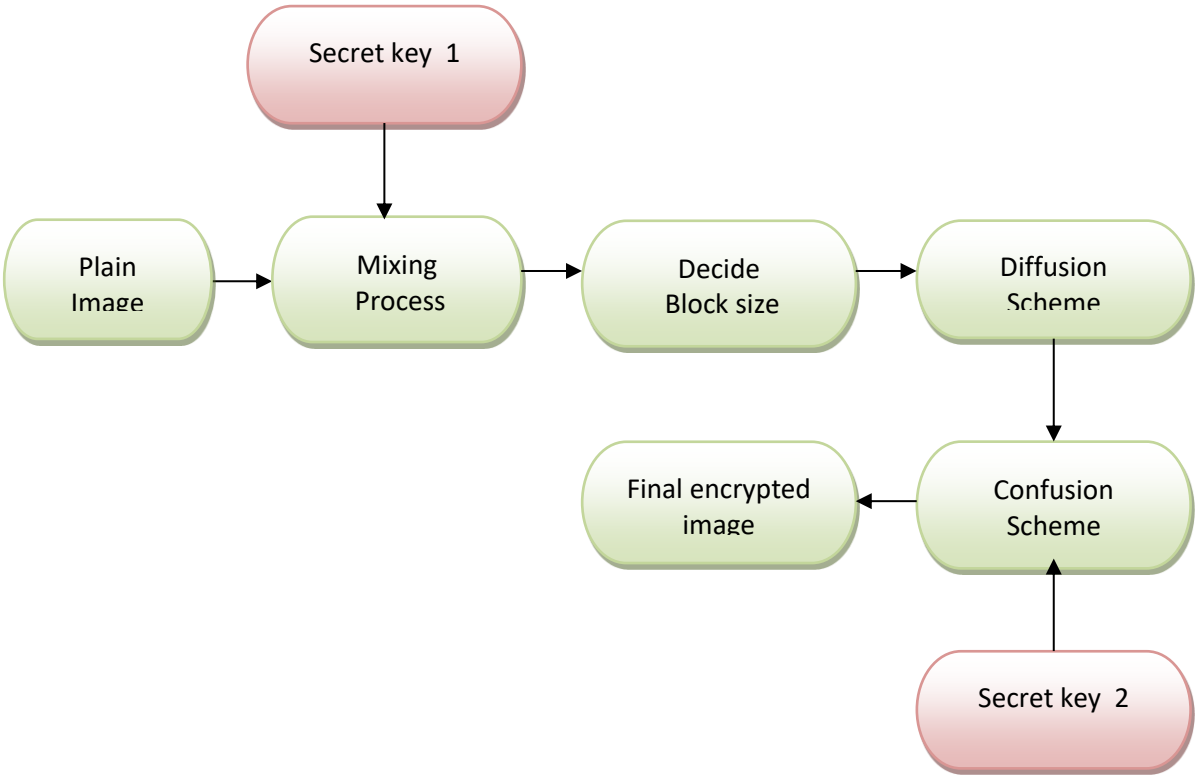


Figure 1: Square Chart of SAIC Encryption Algorithm.

The proposed SAIC algorithm for encryption consists of the following operations:

Step 1: Using the KG algorithm, produce two unique keys.

Step 2: The input image undergoes a mixing process during transmission, degrading the image's quality.

Step 3: we separate the non-overlapping parts of the somewhat jumbled image. The final picture's scale determines how many components will be used.

Step 4: This is to apply the sub-key pair (kx, ky) distribution algorithm on the encoded image. This method is used in the saw-tooth space-filling bend technique to produce a distorted image.

Step 5: The perplexity technique is used to further refine the mixed picture into the final scrambled image.

Step 6: The jumbled squares from Step 6 are assembled into a data file.

A sophisticated public key cryptography algorithm is key generation (KG). KG makes use of both public and private keys. The original photos are encrypted with the open key so that they are illegible. Images encrypted using a public key can be decrypted with a private key. In this case, a pair of public and private keys can be generated by following these steps:

1. Produce a sizable number of random primes m[x, y] and n[x, y].
2. write down s[x, y]=m[x, y]*n[x, y] to record the modulus n.
3. Pick an odd open sort e between '7' and n-1 that is reasonably prime to both m-1 and n-1.

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

4. Using e, m, and n, create a private illustration d, and then register it.
5. Result in (s, e) for the public key and (s, d) for the private key.

To encrypt and decode data, current methods employ symmetric key encryption; nonetheless, the issue of key exchange remains unresolved. This issue can be fixed by using an asymmetric key cryptography method. The primary function of KG in this work is to facilitate the exchange of secret keys; specifically, the public key (s, e) is employed during the mixing procedure, while the private key (s, d) is employed during the unscrambling procedure. Two separate keys are employed in this process to boost encryption speed.

The following is a key aspect of the suggested decoding calculation. The math approach used in unscrambling is identical to that used in encryption, albeit in the opposite order. The Inverse mixing process, Inverse diffusion, and Inverse confusion are the three components of the Secured Asymmetric Image Decipher algorithm. Figure 2 displays a square chart of the suggested unscrambling algorithm.

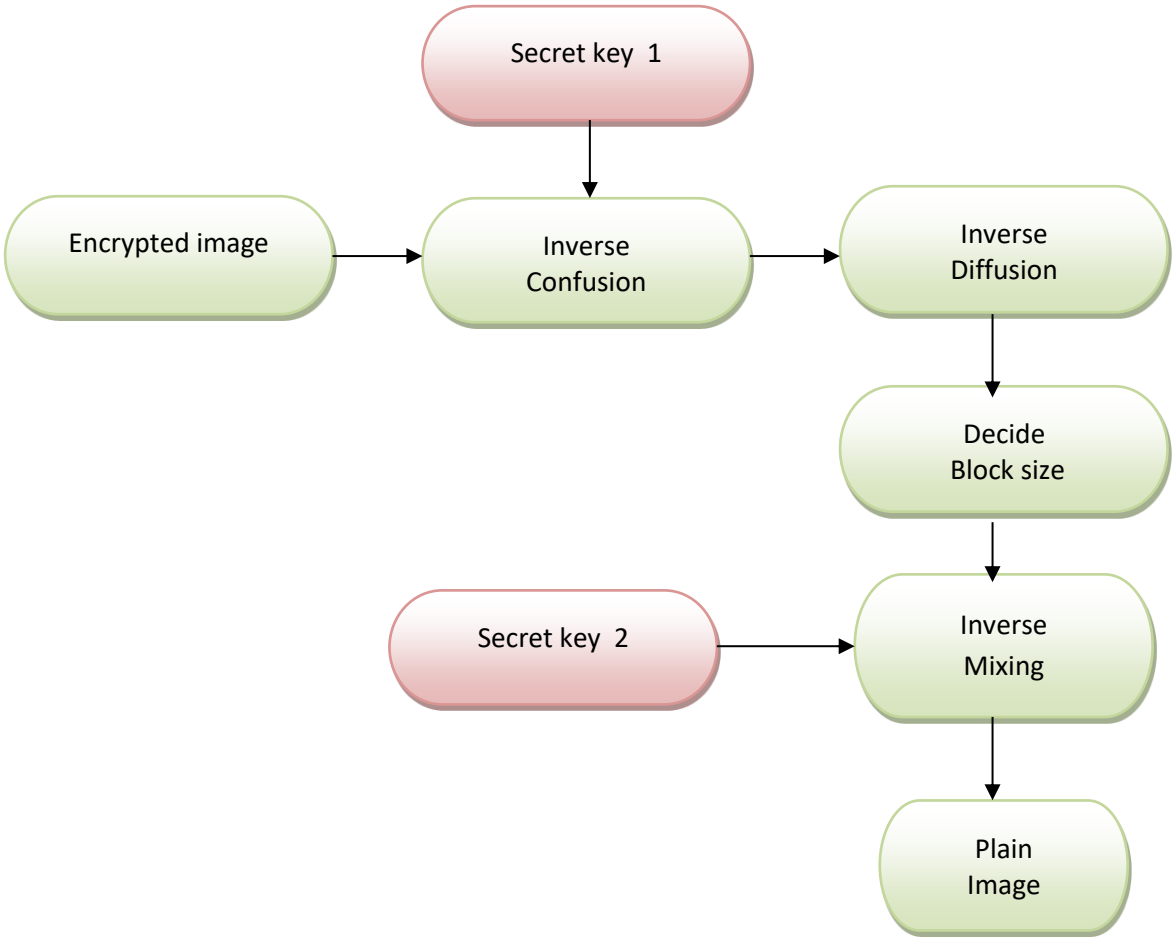


Figure 2: Square Chart of SAIC Decryption Algorithm.

Inverse confusion and diffusion techniques are applied to the encrypted image to produce the decrypted version. In addition, the private key is used in an inverse mixing process on the decrypted picture to obtain the final decrypted image.

4. Result and Discussion:

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

Asymmetric Image Security Measured analysis of the cipher design, such as how well it protects against the most common attacks, is a good example of the kind of careful planning that goes into creating a successful cipher.

4.1. Correlation:

In order to observe the effects of chaos and dispersion in the proposed plan, a relationship analysis is done on the figure picture. In the picture, the connections between nearby elements are stronger than they should be in the figure. In order to assess the link between the two, the accompanying figures are drawn.

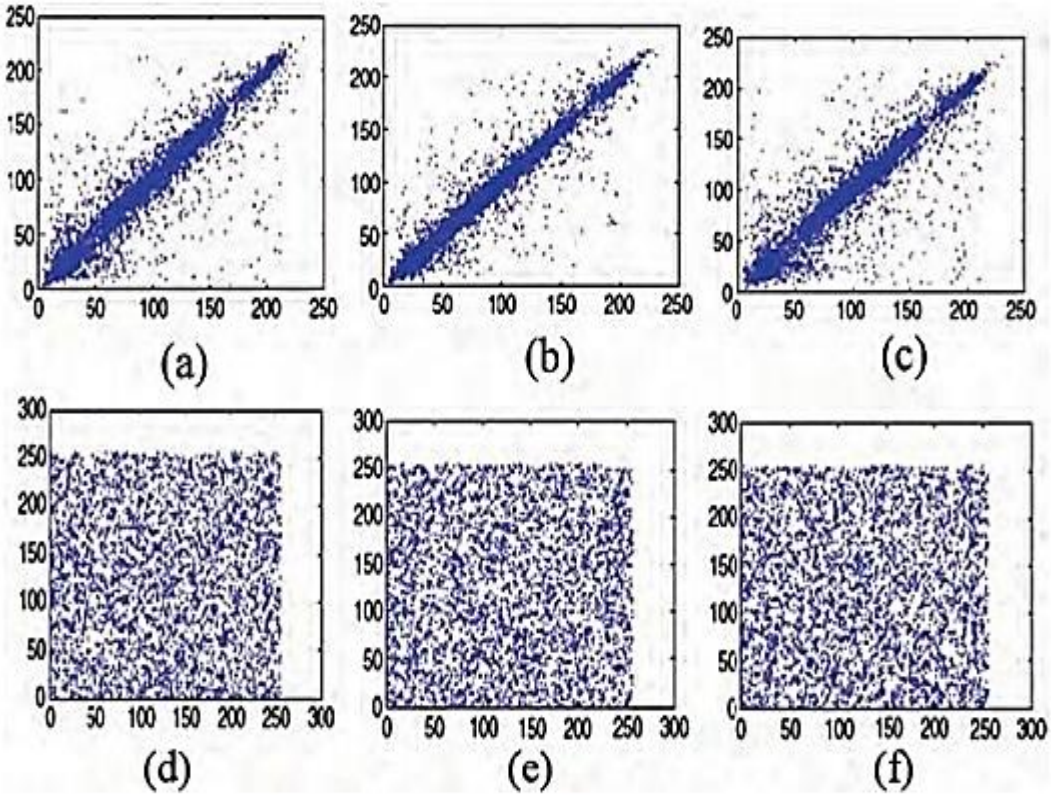


Figure 3: Encrypted images and original images Flat, upright and transverse pixel Spreading.

In Figure 3, we can see how the correlation coefficients for the cipher picture (a, b) are distributed throughout the horizontal, vertical, and diagonal pixels that are next to one another.

4.2. Encryption Time:

The time required for the calculation to encrypt and decrypt a picture is also an important consideration. Using the suggested picture encryption scheme, the times required to encrypt and decrypt a number of different approximated images are determined. The time study was conducted on a computer with an i5 processor and 4 GB of memory. If the value of time is not crucial, then greater focus can be placed on achieving a better level of security. Figure 4 compares and contrasts the times required by various photo encryption algorithms currently in use.

Table 1: Computation Time Analysis of different image data.

S. No.	Test Image	Computation time			
		Tang, Z 2016 [21]	Tao Xiang et. al 2015 [22]	Ting Hu et al 2017 [20]	Proposed approach
1	Spine	2.045	1.437	1.248	0.438

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

2	**Knix**	1.986	1.325	1.024	0.425

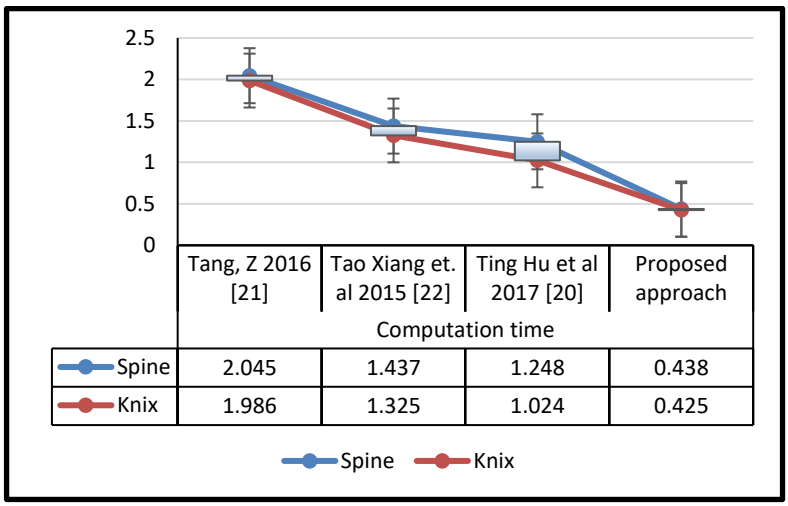


Figure 3: Computation Time Analysis of different image data.

4.3. Dependability Analysis: To determine the efficacy of SAIC's photo encryption scheme, one can use a segment of the Cipher image and the correct unscrambling key. In order to evaluate the impact of the noise attack on the picture encryption plot, we embed the noise into the encoded image in the manner described below.

$$D_j = D\ (k.R + 1) \quad (1)$$

'D' and 'Dj' represent the encoded picture and noisy scrambled picture, respectively; 'k' is a coefficient indicating the degree of commotion; and 'R' refers to random Gaussian data with zero mean and standard deviation.

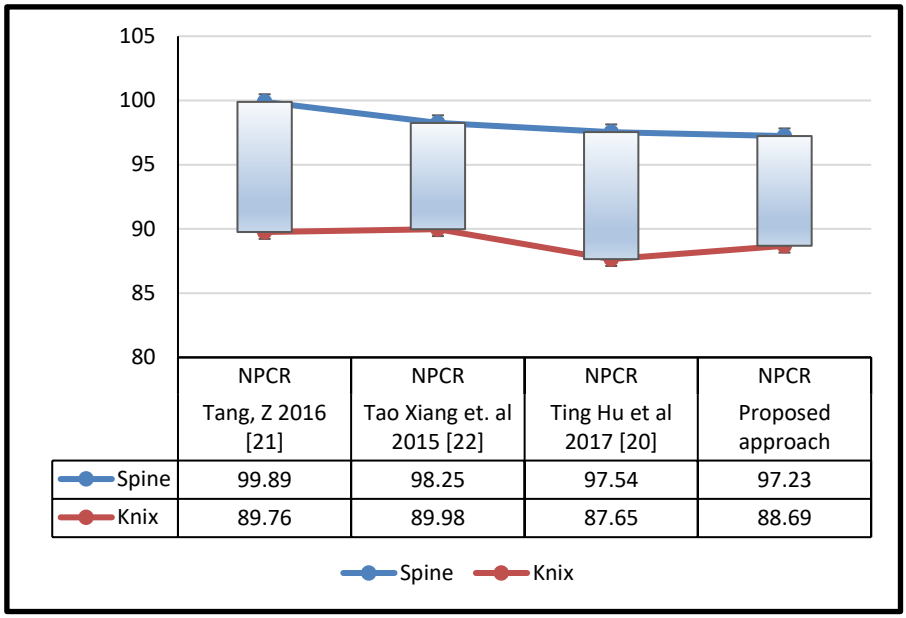
4.4. Plain Image Sensitivity Analysis:

NPCR and UACI are two methods that can be used to assess sensitivity. The NPCR algorithm displays the frequency with which individual pixels in two images have been swapped. The differences between these two images are highlighted by UACI with the usual intensity.

Table 2: NPCR and UACI of various Test Images.

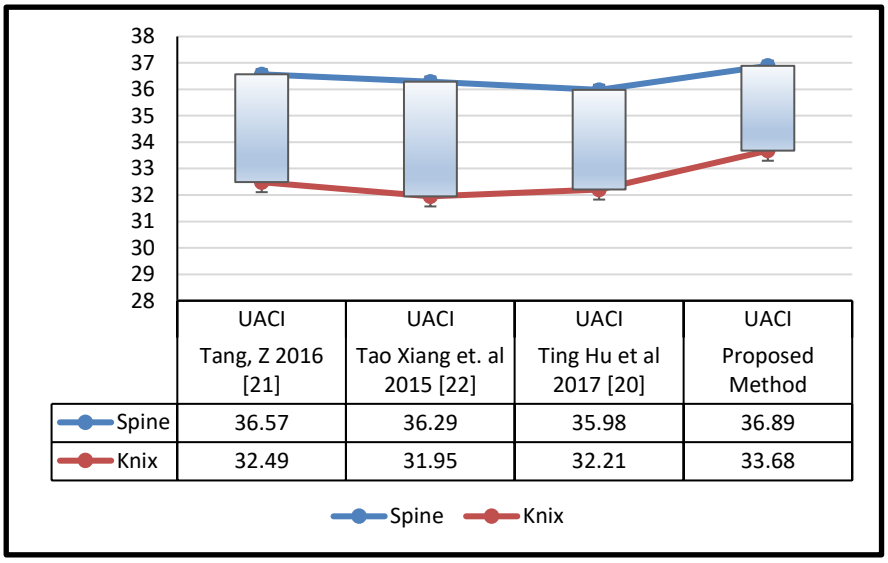
S. No.	**Test Image**	**Tang, Z 2016 [21]**		**Tao Xiang et. al 2015 [22]**		**Ting Hu et al 2017 [20]**		**Proposed approach**	
		NPCR	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**
1	**Spine**	99.89	36.57	98.25	36.29	97.54	35.98	97.23	36.89
2	**Knix**	89.76	32.49	89.98	31.95	87.65	32.21	88.69	33.68

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023



	NPCR Tang, Z 2016 [21]	NPCR Tao Xiang et. al 2015 [22]	NPCR Ting Hu et al 2017 [20]	NPCR Proposed approach
Spine	99.89	98.25	97.54	97.23
Knix	89.76	89.98	87.65	88.69

Figure 4: NPCR Comparison of various Test Images.



	UACI Tang, Z 2016 [21]	UACI Tao Xiang et. al 2015 [22]	UACI Ting Hu et al 2017 [20]	UACI Proposed Method
Spine	36.57	36.29	35.98	36.89
Knix	32.49	31.95	32.21	33.68

Figure 5: UACI Comparison of various Test Images.

It provides more information on the impact that changing the number of iterations and expanding the measurement of the mystery key have on the security that is produced as a result. The use of logical operations in encryption and decryption, along with the asymmetric key system, variable key space, unchanged file size of both the original and encrypted images, and the use of these features in encryption and decryption, are notable improvements in comparison to older techniques. Additionally, satisfying security levels and easy software realization are both benefits of this method.

5. Conclusion:

An ideal image encryption technique should be flexible, secure, and efficient. In this paper, we present an alternative method for the substitution and dissemination process in order to create a simple and efficient Secured Asymmetric Image Cipher (SAIC) Algorithm for grey images. The authors suggest using the Secured Asymmetric Image Cipher (SAIC) Algorithm for grey images since it provides confusion and diffusion qualities

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

and uses two keys within the encryption side itself, so guaranteeing greater security than conventional methods. It describes in greater detail how the resultant security changes if the number of iterations or the size of the mystery key is altered. In comparison to older methods, this one offers significant advancements in terms of both security and ease of software implementation thanks to its key features, which include an asymmetric key system, a variable key space, unchanged file sizes for both the original and encrypted images, and the use of logical operation in encryption and decryption. Despite this, there is still more to be accomplished in this field as a future work research. Some of these recommendations include:

- Using diffusion and confusion techniques, the suggested algorithm can be adapted to incorporate video encryption concepts.
- Higher-dimensional chaotic maps have not been studied mathematically for their chaotic nature.
- Creating a general selective image/video encryption method that achieves all of the above goals is a challenging task. These results for photos should, ideally, also apply to the more computationally intensive problem of protecting videos.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1]. Abdurahman Kadir & Hong Jun Liu 2015, 'Asymmetric color image encryption scheme using 2D discrete-time map', Signal Processing, vol. 113, no. 1, pp. 104 - 112.

[2]. Abitha, KA & Pradeep K Bharathan 2016, 'Secure Communication Based On Rubik's Cube Algorithm And Chaotic Baker Map', International Conference on Emerging Trends in Engineering, Science and Technology, vol. 24, no. 1, pp. 782 - 789.

[3]. Ayesha Kulsoom, Di Xiao Aqeel-ur-Rehman & Syed Ali Abbas 2016, 'An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules', Multimedia Tools and Applications, vol. 75, no. 4, pp. 1-23.

[4]. Baiying Lei & Dong Ni 2014, 'Optimal image watermarking scheme based on chaotic map and quaternion wavelet transform', Nonlinear Dynamics, vol. 78, no. 4, pp. 2897-2907.

[5]. Isha Mehra & Naveen Nischal, K 2015, 'Optical asymmetric image encryption using gyrator wavelet transform', Optics Communications , vol. 354, no. 1, pp. 344-352.

[6]. Iztok Fister & Aleksandra Tepeh 2016, 'Epistatic arithmetic crossover based on Cartesian graph product in Ensemble differential evolution', Elsevier, vol. 283, no. 1, pp. 181-194.

[7]. Jalesh Kumar & Nirmala, S 2015, 'Securing the Contents of Document Images using Knight Moves and Genetic Approach', IEEE, vol. 62, no. 12, pp. 65-73.

[8]. Jalesh, K & Nirmala, S 2016, 'A novel and efficient method based on knight moves for securing the information contents of images a parallel approach', Journal of Information Security and Applications, vol. 30, no. 18, pp. 105-117.

[9]. Kamil Dworak & Michal Kawulok 2016, 'Cryptanalysis of SDES Using Genetic and Memetic Algorithms', Springer, vol. 642, no. 1, pp. 3-14.

[10]. Kekre & Tanuja Sarode, HB 2015, 'Partial Image Scrambling Using Walsh Sequency in Sinusoidal Wavelet Transform Domain', Springer, Intelligent Systems Technologies and Applications, vol. 384, no. 2, pp. 471-484.

[11]. Kunal Kumar Kabi & Arun Chauhan 2015, 'Implementation of New Framework for Image Encryption Using Arnold 3D Cat Map', Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing, vol. 339, no. 1, pp. 379-384.

[12]. Narendra K Pareek & Vinod Patidar 2016, 'Medical image protection using genetic algorithm', Soft computing, Springer, vol. 20, no. 2, pp. 763-772.

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023

[13]. Oh, JY, Yang, DI & Chon, KH 2010, 'A selective encryption algorithm based on AES for medical information', Health Informatics Research, vol. 1, no.5, pp. 22-29.

[14]. Z. Hamici, "Randomness Evaluation of a Genetic Algorithm for Image Encryption: A Signal Processing Approach," arXiv preprint arXiv: 2008.03681, Aug. 2020.

[15]. Saranya, MR & Arun Mohan, K 2015, 'Algorithm for Enhanced Image Security DNA and Genetic Algorithm', IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems, vol. 70, no. 1, pp. 1-7.

[16]. M. Shariatzadeh, M. J. Rostami, and M. Eftekhari, "An Adaptive Image Encryption Scheme Guided by Fuzzy Models," arXiv preprint arXiv: 2208.07825, Aug. 2022.

[17]. Sengul Dogan 2016, 'A new data hiding method based on chaos embedded genetic algorithm for color image', Springer, vol. 46, no. 1, pp. 129 - 143.

[18]. Shihua Zhou & Ziqi Wei 2016, 'An encryption method based on the new secret key algorithm for color image', International Journal of Electronics and Communications, vol. 70, no. 1, pp. 1-7.

[19]. Teng, L, Wang, X & Wang, X 2013, 'Cryptanalysis and improvement of a chaotic system based fragile watermarking scheme', International Journal of Electronics and Communication, vol. 67, no. 6, pp. 540-547.

[20]. Ting Hu, Ye Liu, Li-Hua Gong, Shao-Feng Guo & Hong-Mei Yuan 2017, 'Chaotic image cryptosystem using DNA deletion and DNA insertion', Signal Processing, vol. 134, no. 1, pp. 234-243.

[21]. Tang, Z 2016, 'Multiple- image encryption with bit-plane decomposition and chaotic maps', Optics and Lasers in Engineering, vol. 80, no. 2, pp. 1-11.

[22]. Tao Xiang, Jia Hu & Jianglin Sun 2015, 'Outsourcing chaotic selective image encryption to the cloud with steganography', Digital Signal Processing, vol. 43, no. 4, pp. 28-37.

[23]. Wang, B, Xie, Y & Zhou, C 2016, 'Evaluating the permutation and on operation used in image encryption based on chaotic maps', Optik - International Journal for Light and Electron Optics, vol. 127, no. 7, pp. 3541-3545.

[24]. Wang, GG, Deb, S & Zhao, X 2018, 'A new monarch butterfly optimization with an improved crossover operator', Springer, Operational Research, vol. 18, no. 3, pp. 731-755.

[25]. Wang, X & He, G 2011, 'Cryptanalysis on a novel image encryption method based on total shuffling scheme', Optical Communication, vol. 284, no. 24, pp. 5804-5807.

[26]. Zhao, X, Lin, Q, Chen, J, Wang, X, Yu, J & Ming, Z 2016, 'Optimizing security and quality of service in a real-time database system using multi-objective genetic algorithm', Expert Systems with Applications, vol. 64, no. 1, pp. 11 - 23.

[27]. Shalini Stalin, Vandana Roy, Prashant Kumar Shukla, Atef Zaguia, Mohammad Monirujjaman Khan, Piyush Kumar Shukla, Anurag Jain, "A Machine Learning-Based Big EEG Data Artifact Detection and Wavelet-Based Removal: An Empirical Approach", Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021. https://doi.org/10.1155/2021/2942808.

[28]. Zhengjun Liu & Min Gong 2012, 'Double image encryption by using Arnold transform and discrete fractional angular transform', Optics and Lasers in Engineering, vol. 50, no. 2, pp. 248-255.

[29]. Sui, L.S.; Lu, H.W.; Wang, Z.M.; Sun, Q.D. Double-image encryption using discrete fractional random transform and logistic maps. Opt. Laser Eng. 2014, 56, 1–12.

[30]. Lang, J.; Fu, X.X.; Guo, P. Optical color image asymmetric compressed encryption in fractional Fourier transform domain. Opto-Electron. Eng. 2018, 45, 170732.

Doi : https://doi.org/10.54216/JCIM.120103
Received: December 14, 2022 Revised: February 09, 2023 Accepted: April 27, 2023