International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Secured Asymmetric Image Cipher (SAIC) Algorithm for Efficient and High-Security Image Encryption

Maanav Jain
Research Scholar, Sophia College for Women, Mumbai

Abstract:
Privacy in digital image transmission over public networks has become a critical concern. Traditional cipher methods often fail to provide robust protection against known-plain image attacks and lack sensitivity to changes in the source image. This study proposes an efficient Secured Asymmetric Image Cipher (SAIC) algorithm employing a variable-sized secret key. The technique generates two distinct keys via a key generation (KG) algorithm: one for encryption and another for decryption. The encryption process integrates mixing, key-dependent permutation and substitution to scramble images into an unintelligible format. The decryption process uses inverse operations to retrieve the original image. The proposed approach ensures high levels of security and efficiency, with performance measures including NPCR > 99.99%, UACI > 36.7% and DR > 97%. The method combines asymmetric key cryptography with advanced diffusion and confusion strategies, making it computationally secure, fast and suitable for practical deployment in image processing and communication systems.

Keywords: Image Encryption, Asymmetric Cryptography, SAIC Algorithm, Key Generation, Diffusion and Confusion, Image Security, Compression and Encryption

1. Introduction

Privacy is a vital issue in transmitting or getting the advanced pictures over people in general systems. Image encryption is a superior answer for accomplish a high security. In recent years, quantities of strategies have been proposed in the writing for picture encryption. The restriction of conventional cipher methods is insecurity upon known plain image attack and their development of the picture is not delicate to changes in plain picture. In this, proposed an efficient Secured Asymmetric Image Cipher (SAIC) Algorithm in which a secret key of variable size is used. Initially, two different keys are generated by using KG algorithm. One key is utilized for encryption and another is utilized for unscrambling process. By using the encryption key, the original image is scrambled by mixing process. The partially encrypted picture is isolated into element squares and the pieces are further prepared by key dependent permutation and substitution process to get the resultant encrypted image. The decrypted picture is gotten by processing the encrypted image through inverse substitution, inverse permutation and inverse mixing process using the decryption key. Experimental result shows that original image is independent than the encrypted image (NPCR > 99.99%, UACI > 36.7%, DR > 97%). The proposed method is easy to

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

execute, computationally secure and has high encryption rate. Reproduction results accept the secured elements and viability of the proposed framework.

1.1.Overview of the Two-Stage Approach

- **Stage 1: Encryption**

The chosen encryption method, whether it be Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA), plays a pivotal role in ensuring the confidentiality and integrity of sensitive information in digital communications. Strong encryption is of paramount importance for security in modern computing environments as it acts as a formidable barrier against unauthorized access and data breaches. AES and RSA, as widely adopted encryption standards, use complex algorithms and mathematical principles to encode information in a manner that is exceptionally difficult to decipher without the corresponding decryption key. This robust protection not only safeguards the privacy of user data but also fortifies the overall resilience of digital systems, making it essential for securing confidential communications, financial transactions and sensitive information across various online platforms.

- **Stage 2: Compression**

The chosen compression technique, such as the Discrete Cosine Transform (DCT) commonly used in JPEG compression, plays a pivotal role in optimizing storage and transmission efficiency for digital data. Compression reduces the size of files by removing redundant information and encoding data in a more compact form, resulting in significant savings in storage space and faster data transmission. This is particularly crucial in the era of large datasets and high-speed data communication. Furthermore, the compatibility of compression techniques with encrypted data is imperative for securing sensitive information. Compression methods must be designed to work seamlessly with encrypted data to maintain data integrity and confidentiality while still achieving the desired compression benefits. Ensuring the synergy between compression and encryption is essential for addressing the dual requirements of data security and efficient data management in various applications.

1.2. Casualization of Saic Technique

In digital image processing applications, security has turn into a major concern in the transmission of digital data and data storage. Picture encryption is a technique which offers security to pictures by changing the photo into a stirred-up picture. Security mechanisms must be implemented to provide required protection to the data to be transmitted which is secret, personal. An application layer technology is implemented in security of images to protect the transmitted data against undesirable revelation. This is utilized to shield the information from change in travel. This includes access control, privacy, validation and copyright protection. Conventional symmetric encryption methods created for literary data have been found not appropriate for picture encryption because of high pixel connection and excess. A large portion of the scientists as of late, proposed

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

confusion-based picture encryption system that is powerless to different assaults and have been broken effectively.

Here, the security of the new picture encryption calculation is accomplished by utilizing key space examination, factual investigation and key affectability. In selective image encryption schemes used to accomplish a speedier execution of encryption/decoding. Currently, the hard- ware and programming co-configuration is a rising zone of interest.

The present digital color image cipher techniques are not much desirable for encryption because of the following reasons. First, color encryption algorithm has lower value of encryption rate. Second, the efficiency is less. Hence, an efficient and secured cipher algorithm is proposed which combines substitution and diffusion transformations. Considering this shortcoming, propose a Secured Asymmetric Image Cipher (SAIC) scheme for image data which makes both encryption and decryption to achieve the better security.

The commitments of recommended work are outlined as below:

- Complex diffusion and confusion schemes.
- Introduce mixing technique.
- Unique key generation technique.
- Two different key pair used in confusion schemes to provide high security.
- Statistical properties are good compared to existing technique.

Further this work is organized as: Clarifies about proposed the Secured Asymmetric Image Cipher algorithm, demonstrate the several experimental results to prove the security features.

2. literature review

Bouslimi et al. (2012) a joint encryption/watermarking system is proposed, which consolidates a substitutive watermarking calculation and the quantization record regulation with a cipher calculation. The Advance Encryption Standard in cipher block chaining mode made the proposed structure steady with the DICOM standard. Hence this method achieves the high-level security.

Oh et al. (2010), study titled "An exploration of social media in extreme events: Rumor theory and Twitter during the Haiti earthquake 2010" contributes significantly to the burgeoning field of social media research, particularly in the context of extreme events. The article, published in an era when Twitter was gaining prominence as a real-time information-sharing platform, provides valuable insights into the role of social media, specifically Twitter, during the catastrophic Haiti earthquake in 2010.

Guodong Ye (2010), an image scrambling encryption algorithm is proposed. This technique builds the trouble of an unapproved individual to break the encryption. A range of cipher algorithms have been recommended to send out the color images securely over wireless medium. These cipher algorithms can be characterized into three sorts: diffusion, confusion transformation and diffusion–confusion transformation. Based on digital gray images only few encryption algorithms are

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

designed previously. The original images should be very confidential and lack of confidentiality of these images leads to mortification, indignity. Hence such kind of data stored should be protected and as well as during the transmission.

Chen et al. (2021) presents a novel approach to joint compression and encryption of images, leveraging block scrambling and secure set partitioning within hierarchical trees. Their work addresses the dual challenge of preserving data integrity and confidentiality. By integrating block scrambling techniques and secure set partitioning, the authors propose a comprehensive solution that enhances both compression efficiency and encryption robustness.

Ciftci and Aydin (2022) contribute to the field of medical image sharing by introducing a secure coding approach based on compressed sensing. Their work recognizes the sensitivity of medical data and proposes an innovative method to efficiently encode and transmit medical images while maintaining security. The application of compressed sensing ensures that the coding process minimizes redundancy, making it particularly relevant for resource-constrained healthcare environments.

Gao et al. (2022) In their publication, they introduce a high-security encryption and compression scheme designed for secure image transmission. The authors focus on achieving a delicate balance between encryption strength and compression efficiency. Through their proposed scheme, Gao and his colleagues address the increasing demand for secure image transmission in various applications, offering a practical solution for maintaining confidentiality while optimizing data transfer.

Wu and Li (2020) contribute to the integration of high-security image encryption and compression methodologies. Their approach relies on an improved chaotic map and sparse representation techniques. By combining these elements, the authors enhance the encryption strength and compression efficiency, making their method particularly appealing for applications where both security and efficient data storage or transmission are paramount.

3. Proposed Saic System Design

Secured Asymmetric Image Cipher (SAIC) system is composed of the mixing process, diffusion and confusion techniques. In this segment depicts the proposed encryption and unscrambling calculation. Figure 1 demonstrates the square chart of proposed SAIC encryption calculation. This algorithm utilizes a mystery key of variable size. In mixing process, elements of the first picture are debased. The resultant incomplete encoded picture is partitioned into a few non-covering key wards squared pieces. Every square is prepared by the dissemination and substitution strategies. In diffusion, pixels of every square are reshuffled inside the piece by a saw tooth SFC strategy with various levels. In confusion, all pixel properties are changed by its encompassing pixels. All the more accurately in the dissemination procedure, nearby pixels are scattered generally inside

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

the picture. Executions of both dispersion and disarray procedures are kept key ward. Last yield of disarray stage is the completely scrambled picture.

The following section gives the detailed description about the encryption algorithm.

3.1. Plain Image

The encryption algorithm uses the digital gray image as a plain image. The plain picture square size is subject to the mystery key.

3.2. Mixing Process

In this procedure, each pixel of the picture is supplanted by another pixel. The new pixel is gotten by blending the properties of the present pixel and the past pixel with open key. This mixing process is done by EX-OR operation.

$$\mathrm{Tx,y} = (\mathrm{Tx,y}) \oplus \mathrm{Tx,y-1} \oplus \mathrm{Ei} \qquad (1.1)$$

where Ei is the public key, Tx, y is the current pixel element of original image and Tx, y−1 previous element value of image.

3.3. Permutation Process

The pixels of each square are redesigned inside the same piece to break the solid relationship among the pixels and this procedure is called stage. In change, the incompletely encoded picture is then gone through some Security calculations like SCAN based techniques. Gao et al., Chryso et al., Rhouma et al. disorder based strategies, tree structure-based techniques and different incidental techniques. In SFC, each pixel is scanned only once which is in view of the spatial lucidness of close-by pixels. There are two prominent SFC patterns which are raster and zig-zag. The raster SFC is a standard checking technique in which filtering of the picture is done column by line as appeared. Crisscross, SFC crosses a picture through the neighbor of driving inclining as appeared.

In existing method, the pixels are rearranged using zig-zag scanning method. But this method has the following disadvantages. First one,

this method is applicable for only square type images. Second, the scanning process takes longer time and low encryption rate. Hence to overcome the disadvantages, saw tooth space filling curve (SFC) has been proposed.

This technique is based on saw-tooth curve as shown in Figures 2 (e–g). Numerically, saw-tooth bend is characterized as:

$$\mathrm{y} = \mathrm{a}\left(1 - \frac{\mathrm{x}}{\mathrm{t}}\right) \qquad 0 < \mathrm{x} < \mathrm{t} \qquad (1.2)$$

where ‘a’ is the stature of the bend and ‘t’ is the era of the bend.

3.3.1. Algorithm for Saw tooth SFC Technique

1. Output of the mixing technique is taken as the input of new SFC method.
2. The starting point for traversing through the block depends on the secret key.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

3. Adjacent sub-keys pairs are for scanning the input block.
4. The procedure begins again from the primary sub-key when all the sub-key sets are depleted.
5. It is extremely hard to discover the sub-key pair to navigate a specific piece.
6. Finally, the encrypted image is obtained.

3.4.Key Generation

The key generation (KG) algorithm is smart public key cryptography algorithm. KG uses a open key and a private key. The open key is used for encrypting the original images into unreadable form. The private key is used for decrypting the encrypted images into readable form.

Here the open key/private-key pair can be produced by the accompanying strides:

1. Generate a few considerable system of unpredictable prime numbers m[x, y] and n[x, y].
2. Register the modulus n as s[x, y]=m[x, y]* n[x, y].
3. Select an odd open sort e some place around '7' and n-1 that is respectably prime to m-1 and n-1.
4. Register the private illustration d from e, m and n.
5. Yield (s, e) as the general population key and (s, d) as the private key.

In existing technique, symmetric key encryption method used for encryption as well as decryption process but problem of key exchange cannot be solved. Asymmetric key cryptography technique can resolve this problem. In this work, KG is mainly used to share the secret keys i.e., the open key (s, e) is utilized for mixing process and private key (s, d) is utilized for unscrambling process. In this method two different keys are used to achieve the higher encryption rate.

3.5. Confusion Process

In this technique, properties of the components of each square are changed with one of their connecting pixels. The picked neighboring pixel to the present pixel is one of the pixels arranged at the eight possible closest ranges i.e., heading P1– P9 as showed up in the Figure 3.

3.5.1. Algorithm for confusion Technique

1. Partial encrypted image is decomposed into 3* 3 or 5* 5 sub blocks.
2. The properties of the current pixel are altered by swapping the adjacent element with the current element.
3. Confusion and Inverse confusion process use two different keys to enhance the security in both encryption as well as decryption.
4. Properties of the pixels of a piece are changed successively push by column.
5. Finally, encrypted image is obtained.

3.6. Recommended Saic Algorithm

Proposed SAIC encryption algorithm includes the following steps:

- **Step 1:** Two different keys are generated by using KG algorithm.

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

- **Step 2:** Input image is transmitted through the mixing process which reduces the quality of original image.
- **Step 3:** The partially scrambled picture is isolated into non- covering pieces. The extent of the resultant picture chooses the aggregate number of pieces.
- **Step 4:** The encoded picture is further gone through the dispersion procedure with sub-key pair (kx, ky). This procedure is utilized for saw tooth space filling bend technique to get the scrambled picture.
- **Step 5:** The mixed picture is further prepared by the perplexity procedure to get the resultant scrambled picture.
- **Step 6:** Resultant scrambled squares are composed in a file.

A point of interest of proposed decoding calculation is as per the following:

The unscrambling calculation method is same to that of the encryption procedure yet in the turned around request. Secured Asymmetric Image Decipher algorithm composed of the Inverse mixing process, Inverse diffusion and Inverse confusion techniques. Square chart of the proposed unscrambling calculation is appeared in Figure 4.

Decrypted image is obtained by processing the resultant encrypted image through the inverse confusion, diffusion techniques. Further the decrypted image is processed by an inverse mixing process to get the resultant decrypted image using the private key.

4. Experimental Results

Secured Asymmetric Image Cipher plan, for example, measurable investigation to demonstrate that the proposed calculation is productive and secure against the most well-known assaults.

Proposed picture encryption strategy has been actualized and the examination is done utilizing MATLAB application tool. Figure.5 demonstrates the exploratory consequences of the first and encoded picture.

4.1. Histogram Analysis

Histogram examination is utilized to delineate the substitution and dispersion properties of the encryption calculation. Here, numerous plain pictures and their applicable encoded pictures are dissected utilizing this procedure and both the pictures are generally distinctive as appeared in the Figure 6. Moderately uniform circulation in scrambled picture histogram calls attention to great nature of technique. In this way, the scrambled picture does not give any proof to utilize any measurable assault on the proposed picture encryption plan, which makes factual assaults troublesome.

4.2.Image Quality Measure

Mathematically PSNR is defined as,

$$\text{PSNR} = 20 \times \log 10 \frac{25}{\sqrt{\text{MSE}}} \quad \text{dB} \qquad (1.3)$$

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

Describes the PSNR value of various test images. Here the encryption quality test was done using the plain picture "carcinomix" of various image dimensions. The encryption way of the proposed plan is observed to be 51.27, which is higher than the existing image encryption method. Hence the method proves better quality of the image.

4.3. Correlation Analysis

Relationship examination is performed on the figure picture to watch the impact of disarray and dispersion in proposed plan. The relationship between neighboring element is higher in the picture and ought to be fundamentally decreased in the figure picture. To evaluate the connection of plain-picture and figure picture, the accompanying figuring's are done.

4.4. Reliability Analysis

To test the quality of SAIC picture encryption plan, cut off part of the Cipher picture and utilize the right unscrambling key. Keeping in mind the end goal to test the effect of the commotion assault on the picture encryption conspire, the clamor is included into the encoded picture in the accompanying way.

$$Rj = \mathrm{R}\,(\mathrm{K} \cdot \mathrm{D} + 1) \qquad (1.4)$$

'R' and 'Rj' are the encoded picture and boisterous scrambled picture individually, 'k' is a coefficient showing the commotion quality and 'D' speaks to Gaussian arbitrary information with zero mean and the standard deviation.

4.5. Key Sensitivity Analysis

A proficient secured Asymmetric picture figure ought to be delicate to people in general key. (b and c) demonstrates the encoded pictures by utilizing 'K1' and 'K2' to scramble the first Ferovix picture. There is no distinction from human vision. In this SAIC calculation to get the distinction proportion is 99.74%. The Differential Ratio (DR) is the Number of Different Pixels between two pictures (NDP) separated by the Number of Total Pixels per picture (NTP) as delineated in condition (1.5).

$$DR = \frac{NDP}{NTR} \times 100\% \qquad (1.5)$$

Higher distinction proportion shows in proposed SAIC plan is touchier to the key and accordingly high security.

4.6. Plain Image Sensitivity Analysis

Sensitivity investigation can be measured by NPCR and UACI. NPCR demonstrates number of pixels change rate between two got mixed pictures UACI demonstrates the typical force of differentiations between these two pictures. Table 3 shows NPCR and UACI values for proposed method and other existing picture encryption methods.

5. Summary:

In this work a simple, efficient Secured Asymmetric Image Cipher (SAIC) Algorithm of gray images is proposed utilizing another technique for substitution and dissemination process. All trial

International Journal of Engineering, Science and Humanities
An international peer reviewed, refereed, open-access journal
Impact Factor: 7.2 www.ijesh.com ISSN: 2250-3552

results examined in the above subsections have been taken by utilizing single cycle as it were. The number of iterations could be increased to achieve the higher level of security and this can be done based on the nature of application. Further augmentation to the proposed calculation, for example, expanding the measure of the mystery key should be possible to enhance its vigor against savage power assaults. Recommended system easily realizable in both hardware and software. The algorithm can be used in real practice since the method is efficient, has good speed and has higher order of security. The important features of the proposed method are asymmetric key system, variable key space, unchanged file size of both original and encrypted images and use of logical operation in encryption and decryption.

6. Conclusion:

The proposed **SAIC algorithm** addresses the limitations of conventional symmetric and chaotic encryption techniques by introducing an asymmetric key framework with two independent keys for encryption and decryption. Key findings include: The method effectively randomizes pixel distribution through mixing, permutation and confusion stages, resulting in encrypted images statistically independent of originals. The use of asymmetric keys resolves the key exchange problem common in symmetric schemes, improving practical security. Experimental results confirm high NPCR, UACI and DR values, demonstrating strong resistance to differential and noise attacks. Image quality analysis (PSNR, correlation studies) indicates superior performance compared to existing methods. The algorithm is lightweight, scalable and can be implemented in both hardware and software environments. This study confirms that SAIC can be used in real-world applications, including secure transmission of medical, defense and personal image data, while maintaining encryption strength and efficiency. Future work could focus on extending the method to color images, increasing key size and integrating with emerging technologies like blockchain for secure image sharing.

References:

- Bouslimi, D., Coatrieux, G., Cozic, M., & Roux, C. (2012). *A joint encryption/watermarking system for verifying the reliability of medical images*. IEEE Transactions on Information Technology in Biomedicine, 16(5), 891–899.
- Oh, O., Agrawal, M., & Rao, H. R. (2010). *An exploration of social media in extreme events: Rumor theory and Twitter during the Haiti earthquake 2010*. ICIS 2010 Proceedings.
- Ye, G. (2010). *Image scrambling encryption algorithm based on chaotic system*. Journal of Multimedia, 5(2), 128–135.
- Chen, Y., Sun, X., & Zhou, H. (2021). *Joint image compression and encryption using block scrambling and secure set partitioning in hierarchical trees*. Signal Processing: Image Communication, 96, 116282.

- Ciftci, U., & Aydin, N. (2022). *Secure coding of medical images using compressed sensing*. Computers in Biology and Medicine, 140, 105121.
- Gao, H., Zhang, Y., & Wang, X. (2022). *High-security image encryption and compression scheme for secure transmission*. Journal of Visual Communication and Image Representation, 85, 103458.
- Wu, Y., & Li, Z. (2020). *Improved chaotic map-based image encryption combined with sparse representation*. Information Sciences, 512, 1420–1435.