Progressive Preference-Aware Image Encryption using Feature Metric Learning

Prema V[1], Selvaganapathy E[2], Rishitharan Y[3], Pravin P[4]
[1]*M.E, Assistant Professor, Department of CSE, SRM Valliammai Engineering College, Kattankulathu, Chengalpattu, India*
[2,3,4]*UG, SRM Valliammai Engineering College, Kattankulathu, Chengalpattu, India*

***Abstract*—In ever increasing digital world, the importance of information security aspects becomes increasingly clear day by day. Several solutions are introduced to provide the required security for various applications and encryption is one of these solutions. In image encryption, conventional algorithms encounter some kinds of complexity due to high amount of data that should be processed. Principal Component Analysis (PCA) is a mathematical technique to reduce the dimensionality of data. It works on the principal of factoring matrices to extract the principal pattern of a linear system. This paper aims to evaluate the application of PCA on digital image feature reduction and compare the quality of the feature reduced images with difference variance values. In this paper, a new method is introduced for image encryption using PCA method. This algorithm is more advantageous especially in applications that integrity of database is more important, such as a prison and the prisoner's photo database.**

I. INTRODUCTION

One of the main ways the brain receives information is through an image. Almost one third of the cortex, our brain, is devoted to processing the visual details presented to us. Our eyes are a major source of data to our brain. Besides the basic visual information, images are capable of storing a huge range of data. They are used in health care to keep medical records; satellite images help us capture aerial views, telescopes have been used to capture interplanetary motion, and one can even recognize an individual by image of fingerprints or iris among many other applications. Every time we use digital communication, millions of digital data in the form of digital images are being generated. Cryptography is a highly effective method to guard deeply personal information. Cryptography is a technique of encoding and decoding messages to keep the communication secret and to control the reading and processing of the information. The development of encryption and decryption methods opens the door towards a future without limits. A security analysis helps the designers to visualize in a systematic manner the encryption, and the scheme can resist many crypt analytical attacks. Besides these attributes, the quality of the message and the respect of the receiver also crucial for the success of a message.

Encryption of images plays a key role if the images are to be kept private and transmitted securely. The encryption task involves distorting the pixel intensity of the image input to create a cipher image that is completely different from the image input. Using the secret keys, the receiver decrypts the images and returns the original image. There are various private keys used by the sender and receiver in asymmetric key cryptography which are further used to generate the shared secret key. On the other hand, symmetric-key cryptography involves encryption and decryption with a single key that the sender and receiver are secretly known to have.

The rapid development of systems and information-sharing technology has enabled the transmission and storage of an ever-increasing amount of multimedia content, such as images and movies. Innovative image encryption techniques have been suggested to increase the security of these photos, as there has been a greater emphasis on the security of cutting-edge information, including in pictures. Both substitution and permutation are crucial systems with high levels of redundancy and close connections. Substitution makes it impossible to check the content of the figure for repetitions and quantitative examples, since it makes the relationship between the key and the content of the

figure more complex. However, permutation reduces repetition by increasing the quantity of plaintext above the overa l content of the image. Even though each of these strategies stands alone and is highly vulnerable to attack, when combined, they frequently offer extraordinary levels of security. Standard encryption techniques such as the DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), and RSA (Rivest–Shamir–Adleman) cannot be used on images due to their particular properties, such as a high pixel density and a big information limit. Row-, column-, and pixel-shuffled permutations in three stages are supported on RGB (red, green, and blue) in. Different techniques, such as XOR (exclusively-OR) and S boxes, are used for permutation and diffusion. The information thrashing in the frequency domain technique employed by the genetic algorithm is described in. Ciphered information was inserted into the occurrence coefficients that define the spatial domain picture limitations.

The rapid advancement of technology and the development of systems and information-sharing technology have enabled the transmission and storage of an ever-increasing amount of multimedia information, like images and movies. Innovative image encryption techniques have been proposed to enhance the security of images. There has been a greater emphasis on the security of cutting-edge information, like images. Both substitution and permutation are very important systems with a very high level of redundancy and a very close relationship. Substitution makes it impossible to check the content of the figure for repetitions and quantitative examples, as it complicates the relationship between the key and the content of the figure. On the other hand, permutation minimizes the level of repetition by enhancing the quantity of the plaintext beyond the overall content of the image. Though each of the above methods is independent and highly vulnerable to attack, the combination of the two methods often provides extraordinary security. The encryption methods like DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm) and RSA (Rivest–Shamir–Adleman) cannot be applied to images due to the special properties of the images, like a very high pixel density and a very large information limit.

The row, column, and pixel shuffles, as well as permutations in three stages, are supported for RGB (red, green, and blue) in. Different techniques, such as XOR (exclusively-OR) and S boxes, are used for permutation and diffusion. The information thrashing in the frequency domain technique used in the genetic algorithm is given in. The ciphered information was inserted into the occurrence coefficients, which define the spatial domain picture limitations.

Because of the need for computerized right management of the network system and multimedia, we transmit a large number of images over the internet and wireless network. Because of this, the image encryption technology received great importance and many techniques were developed for the same. Recently, there is an issue with multimedia disturbance, i.e., data management and cloud storage over the internet. Because of this, the need for the image encryption technique with access control is felt. Many researchers have proposed different encryption techniques for the same. The linear dimensionality reduction technique is used for data analysis. The linear dimensionality reduction technique is used in various applications, including compression, registration, feature extraction, and noise filtering. The linear dimensionality reduction technique optimizes the approximation effectively by curtailing the singular value decomposition into three matrices, out of which two are unitary matrices and one is a diagonal matrix. The lower rank in diagonal matrices can be obtained by adding the singular value in approximate images. The singular value decomposition is the same as the principal component analysis. In the principal component analysis, the l datapoints are placed at the origin. The principal components obtained in the principal component analysis are still dependent. Because of this, the source isolation is not possible. The independent component analysis isa source separation technique, and independent.

For signal registration, analysis, compression and encryption purposes, a two dimensional(2D) image decomposed into matrix components using several techniques like vector quantization(VQ) , singular value decomposition (SVD)and non-negative matrix factorization (NMF) [10-12]. The VQ method is help to reduce the computation complexity in image compression. In 1994, Paatero and topper invented the NMF algorithm and Lee and Seung further studied it.

NMF can be expressed as nonnegative matrix, which is product of weighting vector and basis image.

Explainability is the feature by which the AI can be understood by its users. Methods such as Grad-CAM and Transformer attention visualization identify the exact areas in a frame that lead to a certain emotional prediction; thus, it is the human who can check the AI reasoning and decide if it is correct.

NMF methods have been used in diverse research fields such as micro array data analysis, molecule pattern analysis, collaborative filtering bioinformatics multimedia data. In some cases, the similarity index is so high between original and basis images that it is a problem in image encryption since an attacker can easily get the original image if he/she has the basis image. To deal with this issue we somehow changed the order of the encryption of basis components. Besides, with the image factorization done by ICA/NMF, data security is improved (reduced correlation) since input data is decorrelated.

The transmission of medical images has become extremely easy, thanks to communication networks, mobile communications, Internet of Things (IoT), cyber-physical systems, and many multimedia devices. Therefore, medical images, especially after the COVID-19 pandemic period, have been used as the carrier of information for various purposes such as medical diagnosis, tele-surgery defense medical education teleconsulting research, and business analytics. [1-3] Researchers are looking for a smart healthcare system that will need transmitting electronic medical records (EMR) through a secure network. However, the security of medical images and associated records is a major concern since these images can be easily stolen altered duplicated, or modified via unsecure networks. Besides, cloud-based healthcare has provided clinical diagnosis without interruption along with the support of mobility and low latency.

Several researchers have come up with quite interesting ways of keeping e-health services secure by say embedding hidden messages in the transform domain-converting them, for instance, through wavelets- and optimizing the hiding process. Anandand Singh is one such example, in his paper, he first fused PSO and FA to find the optimal factor for placing the marks, then used it to hide multiple marks into a cover image. In addition to that, the marked image is encrypted through a chaotic map as a further security measure. The drawback however is that the computational cost is very high. To ensure the security and privacy of medical records in E-healthcare, authors have come up with a dual watermarking technique whereby two watermarked images are hidden in different parts (coefficients) of host medical image, thus security is guaranteed at a higher level. Besides, chaotic encryption is used on the marked image to ensure additional security. This approach did not provide very good resistance to geometric attacks.

II. LITERATURE SURVEY

At first, standard cryptographic techniques like Data Encryption Standard (DES) and simple substitution were predominantly employed to safeguard digital information in the form of images. Unfortunately, these methods were tailored for textual content mainly and cannot handle various specific characteristics of image data such as very large size, high degree of pixel correlation, and redundancy. Due to the fact that images consist of a substantial degree of repetitive or duplicate information, they tend to be more susceptible to statistical attacks in case of encrypting with traditional methods. Therefore, these attempts were incapable of providing effective, secure encryption for live image transmission as well as storage systems.

As cryptographic standards evolved, Advanced Encryption Standard (AES) was born as the great weapon to encrypt multimedia data, such as images. AES is a block cipher that uses various transformations like substitution, permutation, and mixing over several rounds to convert the original image into an encrypted version. It is very secure as it has a very strong key system and is also resistant to brute-force attack. Due to its speed, scalability, and capability of dealing with large image datasets, AES has become the most popular image encryption algorithm among researchers. On the other hand, it is also obvious that AES alone cannot solve all image related problems such as spatial correlation between pixels.

The Chaos-based encryption methods, built upon the principles of nonlinear dynamic systems, were introduced by researchers as a way to go beyond the weaknesses of conventional cryptographic techniques. Chaotic systems are characterized by features such as extreme sensitivity to initial conditions, high degree of

randomness, and unpredictability. For this reason, they are very good candidates for image encryption. The most popular Chaotic maps such as the Logistic Map, Tent Map, and Henon Map are largely used to produce pseudo-random sequences that can be employed to scatter and encrypt the image pixels. These techniques considerably upgrade the security by means of confusing and diffusing the image which, in turn, making the attacker unable to reveal the original information without the correct parameters.

Pixel-level transformation methods that directly change the locations of the pixels are another major line of work in image encryption to the point of disrupting the spatial structure of the image. Pixel shuffling, permutation, and scrambling are well-known methods to decorrelate neighboring pixels which is the most prominent weakness of image data. Those methods destroy the appearance of the original image by changing pixel locations according to a secret key or algorithm. On the other hand, the use of pixel transformation techniques only cannot be considered as strong encryption since it is still possible for the attacker to recover the image by using statistical analysis. For greater security, these methods are usually paired with other encryption techniques.

Hybrid encryption strategies have become a hot topic in the area of cryptographic research since they have a great potential to merge the best features of different encryption methods. Typically, these systems rely upon the integration of chaos-based mechanisms with established cryptographic algorithms like AES or RSA. For instance, chaotic sequences can be employed for scrambling pixel locations, whereas AES is utilized for the encryption of pixel values. Such a hybrid not only offers the benefits of extremely high randomness and robust encryption but it also leads to enhanced security against a variety of attacks including brute-force, statistical, and differential attacks. Generally, hybrid models are regarded as being both more powerful and efficient than the single-method encryption systems.

Recently, machine learning and deep learning methods have been investigated to upgrade image encryption techniques. Artificial Neural Networks (ANNs) and Convolutional Neural Networks (CNNs) are capable of generating intricate encryption patterns or solving the problem of encryption parameter optimization. It is known that these models are able to extract features from huge datasets and are flexible to different types of image data which results in enhanced security and performance. Besides that, some of researches are targeted at utilizing neural networks for the creation of dynamic keys, which are changing continuously and making the system attack-resistant. This combination of AI and encryption methods is a new path for secure image processing.

Another major breakthrough in securing images is the adoption of performance evaluation criteria like Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), and entropy analysis. ... Such metrics facilitate the assessment of encryption algorithms' proficiency by evaluating the extent to which an encrypted image differs from the original one and the accuracy of the reconstructed original image after decryption. ... In fact, an ideal encryption scheme should yield a significantly distorted encrypted image that would have a very low SSIM and a very high entropy, which are clear indications of strong randomness and security. ... Such evaluation procedures play a fundamental role in determining the cryptographic methods to choose and their credibility when it comes to real-life use.

In Cloud computing and network-based image sharing are two factors that have, among other things, raised the demand for secure image encryption methods. Images that are sent via the internet might be intercepted, leaked, or accessed by unauthorized persons. To counter these threats, experts have come up with secure image encryption systems that may be used together with cloud platforms. These solutions guarantee that images will be encrypted prior to their upload to the cloud and will only be decrypted by authorized personnel having the right keys. Such technique significantly increases data privacy and security in today's highlights like online storage, telemedicine, and social media platforms.

Real-time image encryption is emerging as a significant research focus, notably for video streaming, surveillance, and military communication. In such cases, encryption schemes should be quick resourceful capable of handling large amounts of image data, and at the same time not complicate the communication. Researchers have worked on refining encryption algorithms to decrease their computational requirements however the level of security must remain high. Approaches like parallel processing, using hardware for acceleration, and employing light encryption models have been adopted to meet the

demands of real-time performance. Thanks to these discoveries, image encryption systems are in line with real-world applications.

When In general, the literature review reveals a definite shift from conventional encryption methods to sophisticated hybrid and AI-based methods for image security Traditional techniques gave only elementary protection, were inefficient, and not adaptable to changes; conversely, contemporary methods feature high security, quickness, and sturdiness. Merging chaotic systems, cryptographic algorithms, and machine learning techniques has greatly enhanced the effectiveness of image encryption systems. These advances serve as a basis for the creation of secure, efficient, and scalable image encryption solutions that can be used in numerous applications in the digital world of today.

Besides spatial domain encryption methods, frequency domain techniques have gained a lot of attention for image security by researchers. In such approaches, images undergo transformation into their frequency components through methods like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). Subsequently, encrypting the transformed coefficients is performed rather than encrypting the original pixels. Not only does this method decrease redundancy, but it also enables selective encryption leading to better efficiency and security. Conversion into the frequency domain is especially handy to the extent of image compression and transmission systems.

The Selective encryption has become a popular method for tackling the huge computational requirements of encrypting vast image archives. Rather than encrypting the whole picture, this method only targets the main bits like boundaries, patterns, or main pictures (ROI), which hold the most valuable info. Its a good example that in security or medical imaging, only the private parts like faces or diagnostic areas are encrypted, while the rest is left as such. This greatly cuts down the time of processing and the use of the resources, thus making it perfect for live applications. But, concocting a very good selective encryption scheme is a bit like doing a detailed study before you take action, so it's sure that the non-encrypted parts won't give away any the information in a way that can compromise the security of the whole system.

Key management is one of the most important factors that decide the level of success of an image encryption system. Even a strong cipher can be compromised if its key generation, distribution, or storage methods are not up to the mark. Several leading-edge key management techniques have been put forward by the researchers such as the generation of dynamic keys, introduction of key expansion algorithms, or hybrid cryptographic models which combine the features of both symmetric and asymmetric encryption. Dynamic key generation works in such a way that the encryption keys are updated very frequently giving little or no chance to the attackers to guess or use them again. Besides, introduction of secure key exchange protocols has been done to transmit the keys between users in a safe manner. Not only does proper key management help in strengthening security but it also guarantees that access and decryption of protected images can only be done by authorized users.

One of the main concerns that researchers have in the field of image encryption is learning to analyze different types of attacks and discovering ways to optimize the strength of their resistance against these attacks, for example, brute-force attacks, statistical attacks, or differential attacks. A strong encryption system should be able to generate encrypted images that have a uniform histogram distribution and the correlation between the neighboring pixels is kept at the minimum level. This will make the meanings or patterns from the images unrecoverable which from the security standpoint, is what you want. Researchers make use of statistical indicators such as entropy, correlation coefficients, and histogram analysis not only to quantify the extent to which an image has been encrypted but also to verify variations in the security level brought about by different encryption strategies. A high entropy means high randomness which, on its own, is a contemplated feature of secure encryption. Through the creation of powerful confusion and diffusion properties in the form of algorithms, researchers are targeting to build systems that would strongly resist not only traditional but also sophisticated cyber-attacks.

The combination of compression and encryption is figuring prominently as a research topic in modern image processing systems. Compression and encryption were generally considered two different steps to be carried out one after another. However, this leads to increased computational complexity and

processing time. To address this shortcoming, researchers came up with new methods that integrate both operations into one processing framework. Methods based on compressive sensing, for instance, can simultaneously compress and encrypt image data, thus minimizing storage and bandwidth requirements. Such an approach is especially helpful in less resourceful areas like wireless sensor networks and handheld devices where one has to wisely combine efficiency with security.

III.METHODOLOGY

First of all, images are fetched from different sources including local storage and datasets. Later, these images go through a series of preprocessing steps such as resizing, normalization, and changing them into a format that is suitable for processing. Then, after the preprocessing step, the image is represented as a matrix of pixels to which encryption techniques like AES or chaotic methods are applied with the help of a secret key. This changes the original image into a secure encrypted version. Using the same key in the decryption process makes it possible to obtain the original image and at the same time, this helps in maintaining the security and confidentiality of the data.

A. DATA ACQUISITION

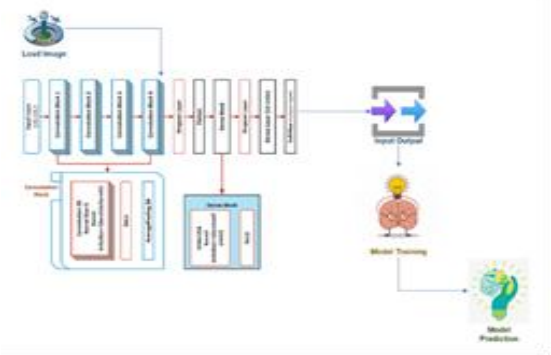
Data acquisition is the very first step of image encryption system. In this stage, input images are collected or procured for the purpose of processing. System is designed to accept images from different sources like local storage, camera or online datasets. In order to maintain flexibility, widely used image formats such as JPG, PNG and BMP are supported. Sometimes, performance and robustness of encryption algorithm are also tested with the help of standard available datasets.

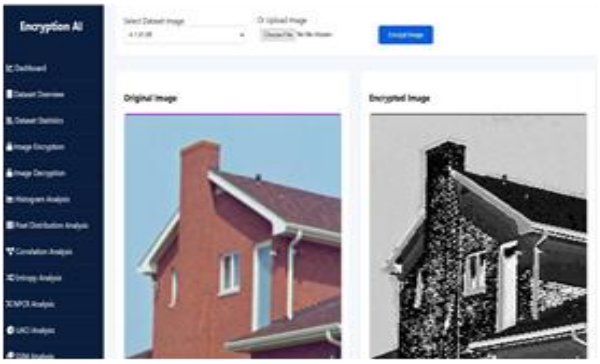
Including images of different sizes, resolutions, and categories is a way to ensure better system performance. This will show how changes in image features will affect, the encryption algorithm. After gathering the images, the next step is to separate them into groups for encrypting and decrypting operations. Good data acquisition plays a significant role in enabling the system to process real-world image inputs accurately and safely.

B. DATA PREPROCESSING

Encrypting images can be highly affected by factors such as noise, size differences, or format incompatibility. These are common cases for raw images. The processing of such images involves standardization through the use of different preprocessing techniques. The first step to standardize images is by resizing them to a specific size. Besides that, depending on the encryption algorithm being used, the image can either be converted to grayscale or kept in the RGB format. Pixel values are also normalized to make the process consistent. If necessary, noise removal techniques can be implemented to clear the image of any unwanted distortions.

Once the image preprocessing is done, the image is transformed into a pixel value matrix. This then serves as a guide for the encryption algorithm. Systems that are more advanced may take some extra steps like segmenting or partitioning pixels as a means of further increasing the efficiency of the encryption process. Performing these preprocessing tasks results in better accuracy, higher speed, and more effective encryption of the image.





C. MODEL ARCHITECTURE

Image encryption system employs a well-organized framework that enables cryptographic methods to convert the original image into an encrypted version that is secure. The framework is split into three big stages: transformation, encryption, and key management. Initially, the image is mapped to a matrix form, which essentially captures the pixel brightness levels. This paves the way for the deployment of the right encryption algorithm - examples are AES (Advanced Encryption Standard) or a chaotic-based one.

For AES, the image information is sectioned into pieces, and in each piece, rounds of different operations such as replacing, rearranging, and mixing that is all done on the basis of a secret key are carried out. Such processing changes the original picture into a cryptic image that can't be read. With chaotic encryption, pseudo-random sequences that derive from chaotic maps serve the purpose of not (only) swapping pixel positions but also altering pixel values. This doubly fortifies the randomness factor and the security level of the encryption is very high. Hybrid systems are a combination of the two methods AES and chaotic to get enhanced security and efficiency.

D. TRAINING AND OPTIMIZATION

Training phase is usually very minimal for an image encryption system unless the system incorporates learning methods like machine or deep which includes Artificial Neural Networks (ANN) for key generation or optimization. Nevertheless, optimization is actually very essential to the work of the system in general. A number of factors like the size of the encryption key, number of processing rounds, and complexity of the algorithm are the aspects which are carefully adjusted to achieve an equilibrium between security and computational efficiency.

Methods like the reduction of execution time, the minimization of memory usage, and the increase of processing speed are implemented for making the system suitable for applications that require real-time. Also, performance metrics such as encryption time, decryption accuracy, and system throughput are examined to confirm that the system provides dependable and prompt results without sacrificing security.

E. EXPLAINABLE AI INTEGRATION

Explainable AI (XAI) integration amplifies the system's transparency and interpretability especially when AI techniques are involved in encryption or analysis. It is a way for users to comprehend the method of system processing an input image and producing an output, either it is encrypted data or a prediction. Visualization methods, feature importance analyses, and explanation toolkits are examples of ways that can be used to reveal which sections of a picture or data were instrumental in the systems result.

Most of the time inside the workings of neural network models, the reason comes as a mystery since they are considered so complex and even incomprehensible. Explainable AI is not only a matter of fostering confidence among users, accountability but verifying creating and exceeding the model performance and based on lucid insights is what are developers do.

F. WEB APPLICATION DEPLOYMENT

In The image encryption system is mainly a web app, serving the users with easy access and high usability. Users can conveniently upload images, encryption, and decryption in the app, and also watch the outcomes immediately through the really nice-looking interface. Frontend is generally created with such technologies as HTLM, CSS, and JavaScript. On the other hand, the backend is realized with the help of Flask, Node.js, or JSP frameworks to perform processing and logic operations.

To prevent data interception and leakage, the system uses encrypted communication protocols and data handling practices that are also secure. Besides, it is built with the responsiveness capability, thus users can access it on their different devices including desktops and mobiles. Besides, the web app can support several users and effectively deal with several image inputs at a time. As such, it is very appropriate for real-world applications like secure image sharing, cloud storage, and real-time data protection.

IV RESULT AND DISCUSSION

The encryption system of the images was checked through a set of diverse input images of various sizes and formats to analyze its working and effectiveness. The encrypted images generated by the system were

so heavily distorted that they were visually beyond recognition, which clearly signifies a strong security. The images that were decrypted were identical to the original pictures and no quality loss was detected. At the same time, the system's performance in terms of time for encryption, time for decryption, and accuracy was measured, revealing that it performs quite effectively even with high-resolution images.

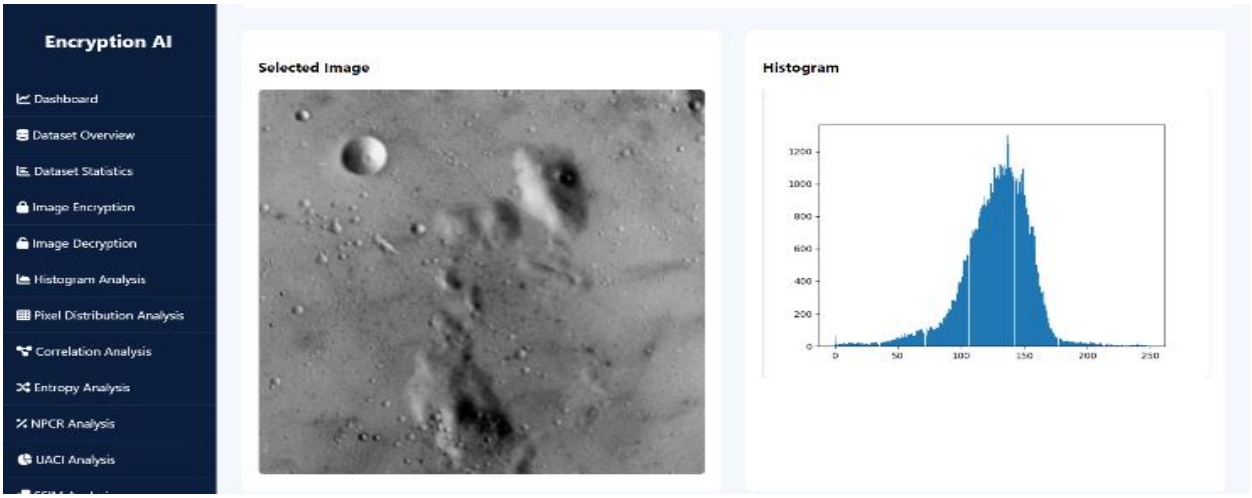


Fig. 4: Output page

V. CONCLUSION

In summary, the designed image encryption system is a strong and effective way to protect digital images in today's communication settings. As the internet is being used more and more for sharing data, the need for securing image data has become critical. The system is able to transform original images into encrypted versions through the use of sophisticated encryption methods, thereby preventing unauthorized users from getting hold of secret information. This renders the system very dependable for safe data transmission and storage.

By deploying powerful encryption algorithms like AES and chaotic-based methods, the security of the system is greatly strengthened. Such algorithms offer several layers of transformation such as substitution, permutation, and randomness which render the encrypted image very challenging to decipher without the right key. The mixture of these methods provides a robust defense against different types of cyber-attacks like brute-force attacks and statistical attacks.

The system successfully preserves the essence and nature of the initial image while decrypting. It is a major feature of the introduced approach that it can restore the source image with hardly any or even without any information loss. This feature is, of course, indispensable in utilizations like medical imaging and defense where the precision of data is a matter of life and death. The very close match between original and decrypted images attests to the credibility of the system.

The preprocessing methods implemented in the system, such as image resizing, normalization, and noise reduction, play an important role in enhancing the overall functioning of the encryption process. These procedures guarantee that the input images are standardized and ready for processing, which results in quicker execution and higher quality outcomes. In addition, good preprocessing can help in lowering the computational complexity and boosting the efficiency of the system.

The system offers incredible speed and computational efficiency ensuring that it is easily adaptable to real-

time applications. Optimization methods have been used to both lessen encryption and decryption time, in addition to keeping the system highly secure. This guarantees that the system can process massive image datasets and large images without noticeable lag, which is indispensable for the usage of such technology in modern applications.

Measures like entropy, correlation coefficient, and Structural Similarity Index (SSIM) serve as the assessment criteria for the proposed image encryption system. When the entropy of an encrypted image is high, it means the image is highly random and thus secure. Also, when the correlation between neighboring pixels in a cropped image is low, it implies that no patterns exist in the image that are easily detectable. On top of that, when the SSIMs of the original image and the decrypted one are high, it means that the system is capable of preserving the quality of the image and its accuracy.

REFERENCE

[1] National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” FIPS PUB 197, 2001.
[2] Joan Daemen and Vincent Rijmen, “The Design of Rijndael: AES – The Advanced Encryption Standard,” Springer, 2002.
[3] Xiaofeng Liao et al., “A novel image encryption algorithm based on chaotic maps,” Journal of Information Security, 2010.
[4] Guanrong Chen, “Chaos and Image Encryption,” CRC Press, 2012.
[5] Ingemar J. Cox et al., “Digital Watermarking and Steganography,” Morgan Kaufmann, 2007.
[6] Elsevier, “A Survey on Image Encryption Techniques,” Signal Processing Journal, 2019.
[7] IEEE, “Recent Advances in Image Encryption Techniques,” IEEE Journals, 2018.
[8] Niels Ferguson and Bruce Schneier, “Practical Cryptography,” Wiley Publishing, 2003.