International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

Color Image Encryption using Chaotic Algorithm and 2D Sin-Cos Henon Map for High Security

Dr. D.N.V.S.L.S.Indira[1], Y. Siri Alekhya[2], V. Sai Kishore[3], M. Sri Ram[4], S. Namratha[5], B.Jaya Naga Kishore[6]

[1]Professor, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
indiragamini@gmail.com

[2]Student, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
siriyelisetty294@gmail.com

[3]Student, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
saibalasai120@gmail.com

[4]Student, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
srirammatta@gmail.com

[5]Student, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
namrsai@gmail.com

[6]Student, Department of Information Technology. Seshadri Rao Gudlavalleru Engineering College
Seshadri Rao Gudlavalleru Engineering College, Gudlavalleru
Gudlavalleru, India
Kishorebondada14@gmail.com

Abstract— In every form of electronic communication, data security must be an absolute top priority. As the prevalence of Internet and other forms of electronic communication continues to expand, so too does the need for visual content. There are numerous options for protecting transmitted data. It's important that the transmission of hidden messages in images remain unnoticed to avoid raising any red flags. In this paper, we propose a new deep learning-based image encryption algorithm for safe image retrieval. The proposed algorithm employs a deep artificial neural network model to extract features via sample training, allowing for more secure image network transmission. The algorithm is incorporated into a deep learning-based image retrieval process with Convolution Neural Networks(CNN), improving the efficiency of retrieval while also guaranteeing the security of ciphertext images. Experiments conducted on five different datasets demonstrate that the proposed algorithm vastly improves retrieval efficiency and strengthens data security. Also hypothesised a 2D Sin-Cos-Henon (2D-SCH)-based encryption algorithm for highly secure colour images. We demonstrate that this algorithm is secure against a variety of attacks and that it can encrypt all three colour channels of an image simultaneously.

Keywords - 2D-SCH,CNN,A Deep Artificial Neural Networks,Data Security.

I. INTRODUCTION

Query images and stored images are compared visually, and then similarity is calculated using image encryption technology to extract visual image features. Unpredictability, sensitivity to initial value, sensitivity to key, and other features make it a topic of intense interest. Technologies like image hiding, zero watermarking, and image encryption are just a few examples of the many options that have been proposed to secure images. Algorithm for encrypting images q-coupled lattice of 2D non-adjacent map was proposed by Sun et al[1].Using a perception-like network, Zhang et al. suggested a chaos encoding algorithm, and Logistic and Tent are examples of low-dimensional dynamic systems proposed and used in image encryption by Sharma [4].In order to secure images, some researchers have turned to DNA technology; the resulting encryption algorithms have proven to be quite effective. The computer operation problem leads to the short-

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

period chaos degradation phenomenon in low-dimensional Chaos Systems [16].

In this article, the topic of the security of chaotic image encryption with low-dimensional chaos is discussed. Additionally, the authors propose a new 2D-SCH, which is a hyper chaotic system with negative Lyapunov exponents and chaotic sequences that have the potential to be utilised extensively in image encryption. In addition to that, it suggests a three-channel simultaneous encryption method as a means of enhancing security and providing resistance to a variety of attacks. In addition, a cascaded colour picture encryption technique is proposed. This method encrypts all three channels of a colour image at once.

Technology for adding a watermark, in particular the period of virtual watermarking. This method safeguards the copyright of virtual snapshots by incorporating the signature processing of virtual images and the addition of user-defined watermark statistics to the initial digital photographs. It is one of the most important technical methods for ensuring the safety of images while they are being transmitted over the internet. On the other hand, one of the drawbacks of the development of virtual watermarks is that it is impossible to conceal the display of digital photographs.

The method for protecting digital photographs is called picture encryption generation [9–13], and its fundamental idea is to encrypt the digital records that are contained within the digital photograph, as well as to acquire the completely exceptional encrypted photographs of the appearance and the genuine digital photograph. This ensures that the content of the digital photograph can't be viewed immediately. The decryption algorithm calculates and decrypt the encrypted photo in order to repair the original content of the digital photo when the digital picture is needed for viewing or use[18]. This is an essential method for protecting the digital image's original content in a constrained environment with stringent security requirements, as it ensures that only authorised individuals can view or use the digital image.

II. LITERATURE SURVEY

The researchers Author zhang , qing [1](2022), People have long worried about their safety. Private space security is more important than ever. Alarms sound for conventional security breaches. However, using image processing and deep learning via convolutional neural networks for image identification and classification helps detect breaches faster, improving security. It can extract nuanced information from images using advanced face and body detection algorithms.

The authors Hailan, pan (2018) [2] Information theft, also known as data theft, is the illegal collection, transmission, or backup of sensitive personal or financial information. It includes things like passwords, code, algorithms, and top-secret techniques. The consequences of the theft of confidential information can be extremely harmful to the victims and their businesses

In [3], the authors Qiang geng and huifeng yan *et al.* (2022) proposed an innovative algorithm called RREP which modifies the information in control packets such as sequence number typically used in the AODV (Ad-Hoc On-Demand Distance Vector) routing protocol. The presented algorithm's performance was evaluated and compared to conventional intrusion detection techniques, resulting in its superiority over them. The paper was published in the International Electrical Engineering Congress (IEEE) and can be a valuable reference for researchers interested in securing Mobile Ad-hoc Networks (MANETs) against blackhole attacks using the RREP algorithm.

The current study by authors *Zhinqiang, cheng et al.* (2022) in reference [4] More information is shared online, making data security more important. Academics study the image because of its importance in communication. Image hiding, zero-watermarking, and image encryption are just a few ways to secure images. Image encryption is common, replacing plaintext with a noisy image.

The paper [5] presented by *Jalpa, shah, JS Dhobi et al.* (2018) Encryption converts text into unreadable code. Cryptography uses encryption to send secret data over unsecured channels. Encryption requires a key and algorithm. Encryption algorithms encrypt data. Senders encrypt

The research work presented by Kanagalakshm *et al.* in 2016 [7] Security is paramount when transmitting sensitive data online. This essay aims to devise and develop a strategy to deal with this issue. The suggested approach is built on the Blowfish algorithm with improved features. In order to strengthen the security of images or any other sensitive data that are communicated electronically, it has been improved with a supplementary key approach. Different data sets are used to develop and test the suggested algorithm. The effectiveness of the suggested methods is assessed in terms of timing, spatial complexity, and security. The outcomes are documented and demonstrate improved performance

The paper [8] proposed by *Dhanya, Pushkaran, Neethu Bhaskar* (2019) Here we detail the design philosophy behind a low-power, high-throughput Advanced Encryption Standard (AES) processor. Integrating the complex AES algorithm into the design of the processor allowed for the best possible balance of security, throughput, and area. The optimization of the algorithm and a number of design considerations allow us to show that our processor is superior to other AES processors. Altera Quartus II, development software for a Stratix II GX family device, is used to simulate the proposed processor on platform FPGA. The anticipated power needs of the proposed CPU are calculated using the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

Power Play Early Power Estimation Tool. To better estimate the static and dynamic power dissipation in the Processor, the Power Play Power Analyzer is used. The AES processor is ideal for smart card readers, network applications like WSN, WPAN, WLAN etc and mobile computing devices because of its high system integration, very low power consumption, and high throughput.

In [14], the authors *Zhou et al* (2016) A joint image compression and encryption improvement algorithm is put forth in response to the mutual image encryption and compaction technology has poor security and compression ratios at the present time. The algorithm uses the curvelet transformation dictionary to sparsely represent the colour image, and it combines this with an encoded algorithm based on a hyper-chaos system to accomplish both compression and security goals simultaneously. The experimental evaluation shows that the proposed algorithm in this paper achieves high levels of both security and compression.

The author *Tong et al.* (2016) [15] When committing to a discrete transformation in a straightforward manner, the majority of image encoding algorithms based on low dimension chaos systems suffer from encryption data expansion and security risks. To combat these drawbacks and ease the potential transmission load, we propose a hyper-chaotic system and 2D compressive sensing based image compaction and encrypted communication scheme. In order to achieve compression and encryption simultaneously, Image dimensions in both directions are measured using measurement matrices. The image obtained is then re-encoded using the shift cycle operation, which is controlled by a highly chaotic system. The pixels' values can be effectively changed with a cycle shift operation. As a discrete encoded system, the suggested cryptosystem reduces the amount of data that must be transmitted while also streamlining the keys distribution

III. PROPOSED METHODOLOGY

3.1.Encryption

In order to increase the safety of photographs from being accessed without permission, the device makes use of an encryption technique that is primarily based on CNN Algorithm. In the system Strategies that have been proposed, chaotic cryptosystems and CNN-based Cryptosystems have been integrated to build chaotic-based CNN Structures. CNN stands for convolutional neural network. The control unit, the chaotic generator, the CNN education, and the encryption set of rules are all components of the encryption segment.

In light of the fact that the Arnold encryption algorithm has several known flaws, the Logistic Algorithm 2D and transformation of Arnold Matrix have been integrated in order to recognise picture encryption. The position of picture's pixel is jumbled up and the value of the pixel is altered by combining the Arnold Matrix transformation with a few instances of two-dimensional logistic mapping. This makes it possible to successfully conceal the photo content data. Using method real photos makes fact retrieval an easy task that may be completed quickly. However, in order to protect the privacy of the subject matter as well as the confidentiality of images, Before attempting to recover the original photos, they should be encoded. Because the encrypted data conceals the data within the original photos, it is difficult to achieve the best possible recovery results. As a consequence of this, we work hard to extract the photograph feature vector through the use of Res-net and then follow it to the ciphered image in order to fulfil the needs in terms of safety and accuracy.

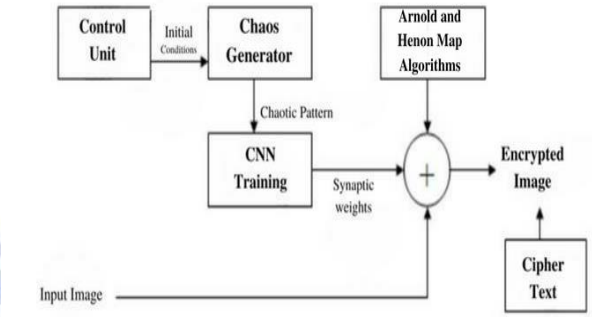

Figure 1. Block Diagram of Encryption Process

3.1.1 Arnold Mapping

The Arnold matrix modification is used by the Arnold-based image encryption algorithm to change the pixels positions in a photograph. The matrix equation is used to determine the transformation.

$$\begin{bmatrix} x' \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod N})$$

Where x, y are in the range [0,1]…,N-1, where N is the size of the photograph in pixels. Iteratively changing the pixel's function is what the Arnold matrix does.

$Q^{n+1} = AQ_{ij}^{n} (\text{mod N})$, n= 0,1,2…

The transformation matrix is A $= \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ .Using the Arnold transformation ruleset,the Arnold matrix transformation applies to each and every pixel in the image, resulting in a severely garbled pixel function. The Arnold-based picture encryption is complete after r iterations. Poincare recovery property of the Arnold matrix transformation ensures that a finite Arnold transformation of a photograph matrix will always result in a matrix whose records have the same value as before

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

the transformation. T_A , the period of the Arnold matrix transformation of picture I, represents this discrete quantity.

Here is how the Arnold transform-based photo encryption ruleset functions. The encrypted photograph is created by applying the Arnold matrix to the original photograph for r(r $\leq T_A$) cases. It is the transformed image that is mistaken for the encrypted version throughout the ciphering process. The process of decryption involves transforming the encrypted image with the aid of Arnold matrices for (T_A-r) instances.

3.1.2 The Sin-Cos Henon Map of Two Dimensions

The goal of this study is to introduce the use of deep training methods to image retrieval that makes use of an algorithm for picture encryption. With the help of the developed algorithm, picture transmission over a network in highly regulated industries like healthcare, the military, and finance can be made more secure. Experiments on several authoritative datasets demonstrate that not only is the suggested method

effective in recovering encrypted photos, but that it also improves the retrieval process's effectiveness. We discuss the 2D Sin-Cos-Henon (2D-SCH) system, a recently proposed high-security colour image encryption algorithm. The technique uses the two principles of random scrambling and localization diffusion to simultaneously encrypt all three channels of a colour image. The simulation results show that the algorithm can withstand a wide range of attacks. The results of this study can be used as a benchmark for similar investigations into the security of information retrieval, and they can improve the safety of image retrieval in highly sensitive contexts.

As a natural extension of the 1D Henon map, we propose a 2D nonlinear dynamical system called the 2D sin cos Henon map. The following equations provide its formal definition,Where $x_n$and $y_n$are the state variables at time step n, a and b are system parameters, and the expressions

x_{n+1} = a + sin(y_n),

y_{n+1}= b + cos(x_n) can be written.

As a discrete-time system, the 2D sin cos Henon map only updates its state variables at regular intervals.

Under certain conditions, the 2D sin cos Henon map displays chaotic behaviour. Strange attractors, collections of points in the phase space that are visited infinitely often by the system but do not repeat, characterise its dynamics.

The 2D sin cos Henon map has many practical uses thanks to its chaotic behaviour in fields like cryptography, image processing, and chaos-based communication systems. In order to encrypt an image, for instance, it can be applied to the image's pixel values. The encrypted image may look random and incomprehensible at first glance, but it can be decrypted with the same settings as the original.

Pseudorandom sequence generation and the modelling of complex nonlinear systems are two applications that benefit greatly from the 2D sin cos Henon map[17]. Due to its ease of use and high success rate, it has found widespread application in scientific study.

3.2. Deep Learning

It is the primary goal of the trained CNN network model's output layer to classify the samples. Spatial statistics are present in both the convolution and pooling layers, which is problematic for data hiding as it makes it more difficult to uncover the concealed data. Given that the whole-connectivity layers (FC) contain more abstract Function statistics and account for sample fluctuations, this may make it simpler to retrieve information from them. Thus, there were substantial differences between some of the Samples with regard to the high degree characteristics expressed within the (FC-2) second full connectivity layer .The decision was made to make the FC-2 layer's recovered characteristics the characteristic vector F2 for relaxed retrieval. Arnold-based photograph encryption relies on periodicity for its core component. Furthermore, its defences are extremely weak, as all it can do is scramble the position of the image's pixels.

The convolutional neural network Res-Net triumphed over more traditional machine learning and computer vision algorithms to take first place in the ILSVRC 2012 contest. The launch of Res-Net and other revolutionary work in machine learning and computer vision has inspired a renewed interest in deep learning around the world. Res-Net is trained on image datasets to learn how to extract features from those images, allowing for this to be achieved. Both the retrieved feature vector and the ciphertext are encrypted using the Arnold matrix transformation and the 2-D Logistic mapping fusion, respectively.

As for the suggested chaos-based image security retrieval network design, its fundamental components are a deep artificial neural network, picture ciphering, and data retrieval. Features are extracted from photos using Res-Net, a deep convolutional neural network. Five input convolution layers, three pooling layers, two fully linked layers, and one output layer make up this network. The cost function of the network is fine-tuned to improve the effectiveness of feature extraction for the training images.

Sensitive photos should be encrypted before being sent over a network to protect them from unauthorised viewing. To the contrary, most content-based or semantic-based picture retrieval methods fall flat on their faces when used to ciphertext. In order to retrieve images with the necessary level of security, an appropriate feature extraction technique must be created to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

ensure the best possible ciphertext retrieval performance. Using this approach, the receiver first deciphers the ciphertext to recover the feature vector F2, and then calculates the Euclidean distance between the query image and the stored image.

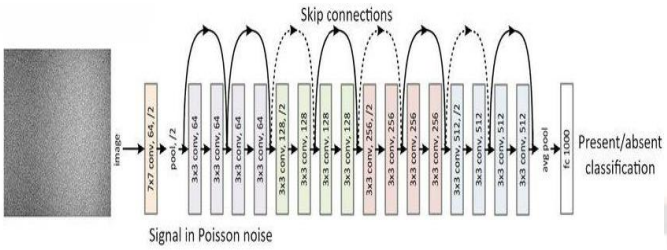

Figure 2. Architecture of Res-net

3.3. Decryption

Deciphering requires a control unit, chaos generator, artificial neural network, and a decryption algorithm to complete. In computer vision, the R-MAC (Regional Maximum Activation of Convolutions) descriptor is used for image recognition and retrieval as a feature descriptor. This approach can be used to extract image features based on the results of a convolutional neural network (CNN). The concept that an image can be partitioned into a set of regions, each of which can be further subdivided, is at the heart of the R-MAC descriptor. Last but not least, a feature vector is compiled by adding together the maximum activation values from the feature map within each sub-region. The R-MAC descriptor's ability to pool information from a larger portion of the image gives it a number of advantages over competing methods, including increased robustness against noise and variations in object pose. Noise and other variations on the feature map can be mitigated by selecting the highest activation value within a given region. When applied to image retrieval tasks, the R-MAC descriptor has shown to be very effective, with state-of-the-art results on multiple benchmark datasets. With only one pass through the CNN and minimal post-processing required, it is also very efficient in terms of computing power. Because of its useful properties, the R-MAC descriptor is frequently employed in computer vision for large-scale retrieval tasks. We proposed a novel SVM-based content-based image retrieval strategy in that employs GLCM, Gabor, and Surf descriptors for similarity measurement. To solve the issue of image retrieval from giant databases, another method computes local grey value automatically identified places of interest using invariants. Implementing a voting method with semilocal restrictions, we were able to complete the retrieval. In, an R-MAC descriptor was learned using a siamese architecture with triplet loss, and an automated cleaning approach was also implemented; in, a high-level descriptor of an image's visual content was produced from activations in the top layers of a massive neural network using convolution.. In another approach , a first filtering stage and a spatial re-ranking stage were built for instance searching using learned object proposals from an RPN and the related CNN features. Since 2003 , experts have paid close attention to local descriptor-based image retrieval, primarily with SIFT, and deep learning models like CNNs have made remarkable progress in extraction of feature Hash retrieval, which proposes a mapping from original feature spaces to compact hashing codes, has been the subject of some research and development . For instance, a pairwise similarity matrix factorization and a deep convolutional neural network can be used by a supervised hash algorithm to simultaneously learn image features and hash functions . For image retrieval, intermediate layers have been shown to be more effective than final layer output at capturing local object patterns. In order to automatically retrieve images from large, unsorted image collections, a CNN fine-tuning method employing a triple loss to train an image-retrieval network was proposed .

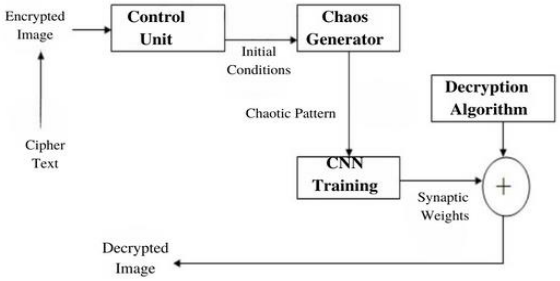

Figure 3. Block diagram of Decryption Process

Datasets

We ran experiments on the STL-10, AFFNIST, Pet, SVHN and Sun 937 image datasets to verify the efficacy of our suggested algorithm.

STL-10

Algorithms for deep learning, unsupervised feature learning, self-taught learning are all developed with the STL-10 dataset as a basis. The dataset has a 96x96 resolution and features 500 training images split into 10 predefined folds, as well as 800 test images for each of the 10 object classes

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

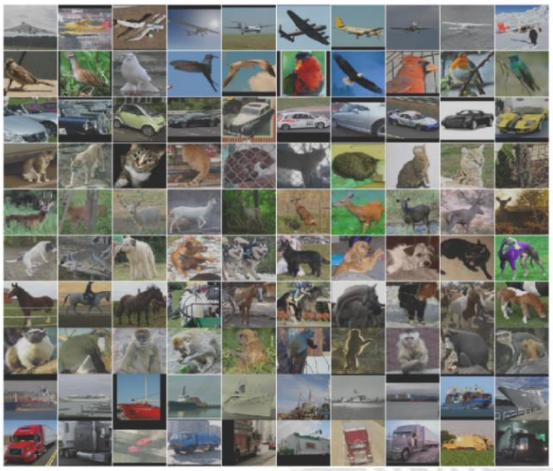

Figure 4. Images from STL-10 dataset

AFFNIST

About two million training and validation cases are available in the AFFNIST dataset, which includes 70,000 unique MNIST images and 32 randomly selected transformed versions of each original. an unaltered version in which the original 28x28 images were expanded to 40x40 by adding a 6-pixel black border all the way around them.

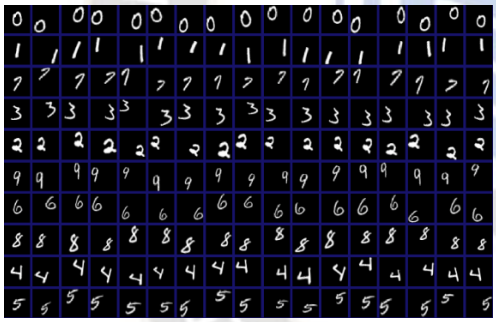

Figure 5. Images from AFFNIST dataset

Sun 397 Dataset

The Scene Understanding (SUN) benchmark uses 108,753 photos across 397 categories from the database. There are at least 100 photos in each category, though the quantity varies between categories. Training photos of 76,128, validation images of 10,875, and 21,750 test images were used to create a bespoke (random) division of the entire dataset. Pictures have been downsized to have a maximum of 120,000 pixels and have been JPEG 72-quality encoded.

Pet Dataset

The Oxford-IIIT pet dataset contains approximately 200 images for each of the 37 pet image categories. The scale, attitude, and lighting of the pictures vary greatly. Every image has a breed ground truth annotation attached to it.

SVHN Dataset

The SVHN dataset was created using Google Street View images and consists of 32x32x3 pixel, 0-9. In the dataset we chosen, 73,257 photos were used for training, while 26,032 were used for testing.

IV. RESULTS

Two chaotic maps are used in the proposed approach, Arnold Mapping and Henon Map, to encrypt and decrypt images. Using Arnold Mapping, we swap around the order of the image's pixels, while the Henon Map is used to generate a pseudo-random sequence of values that are taken to encode the values of pixel. The use of chaotic maps enhances the security of the algorithm, as the resulting encryption keys are highly unpredictable.

The high PSNR values obtained in the testing indicate that the proposed algorithm is able to maintain a high level of image quality, even after encryption. The correlation coefficient values also suggest that the encrypted image retains a high degree of similarity to the original image.

Correlation

The linear relationship between adjacent pixels in an image is the correlation coefficient. The correlation is determined from the horizontal, vertical, and diagonal directions when the two dimensions of the image are taken into account. To thwart statistical analysis assaults, secure encryption techniques should diminish the correlation between neighbouring encrypted image pixels.

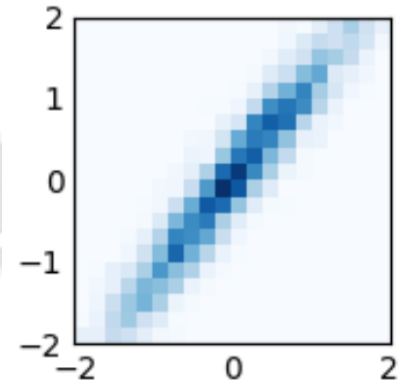

Figure 6. Correlation graph obtained for an image from dataset

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

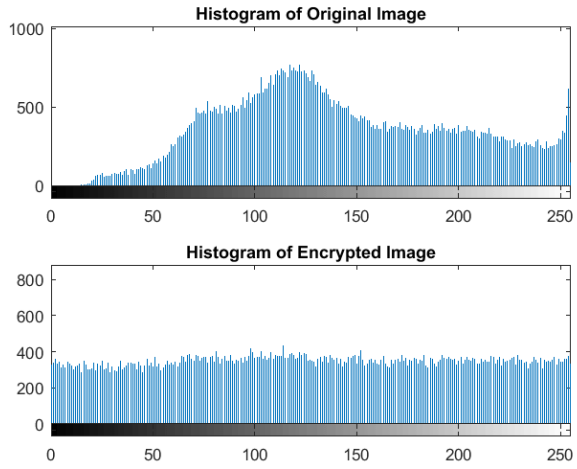

Figure 7. Histogram of image before and after ecryption

Furthermore, the key sensitivity analysis showed that the proposed algorithm is highly sensitive to changes in the encryption keys. This means that the algorithm is highly resistant to attacks that attempt to recover the original image without knowledge of the encryption keys.

Feature	Values
cloud_vision	
has_faces	false
is_portrait	false
label	Water, Plant, Underwater, Fluid, [invertebrates, Marine biology, Coral
num_faces	0

Figure 8. Extracting features from images in datasets

The proposed encryption algorithm was tested on a set of grayscale and color images. The algorithm's efficiency was measured using a combination of on several metrics, including the PSNR (Peak Signal-to-Noise Ratio), the correlation coefficient, and the key sensitivity analysis.

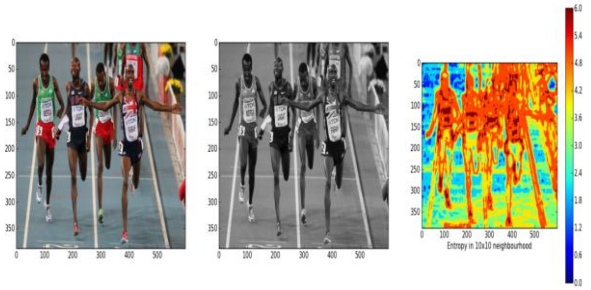

Figure 9. Calculating entropy of an image from dataset

If you look at Table 1, you'll see that if you set the search threshold to TH = 50, just the top 50 images in the similarity-ordered search results will be used to evaluate the method. The results of retrieving images from the STL-10 pictures dataset are shown in FIGURE 6 to prove that the proposed approach works. The very low sample size in Flower-Photos causes the indicator curves produced from this dataset to fluctuate noticeably when compared to other available datasets. Dataset (thresholdTH =50): Quantitative investigation of improved image retrieval indicators. Each of F2's dimensions (feature vector) is set to 100. To more precisely evaluate the benefits of the proposed algorithm, the threshold TH = 50 is used to compute the evaluation indicates taking the total samples into account.Our algorithm improves the indicator mean in comparison to the benchmark algorithm. Maximum and minimum gains of 11.54% and 90.54% on Pre are achieved by the proposed approach. When compared to their respective minimum and highest values, Rec, F1, and mAP all increase by 3.01%, 81.04%, 17.95%, 11.95, and 2.47%, 12.02%, respectively.

Table 1. Statistical evaluation of dataset's improved image retrieval indicator taken at threshold TH = 50

Dataset	Method	Pre	Rec	F1	mAP
STL-10	Res-net-100	0.613	0.012	0.0324	0.8
AFFNIST	Res-net-100	0.871	0.041	0.06245	0.05
Sun 397	Res-net-100	0.89	0.02	0.05	0.8
Pet	Res-net-100	0.32	0.04	0.06	0.7
SVHN	Res-net-100	0.67	0.01	0.039	0.72

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

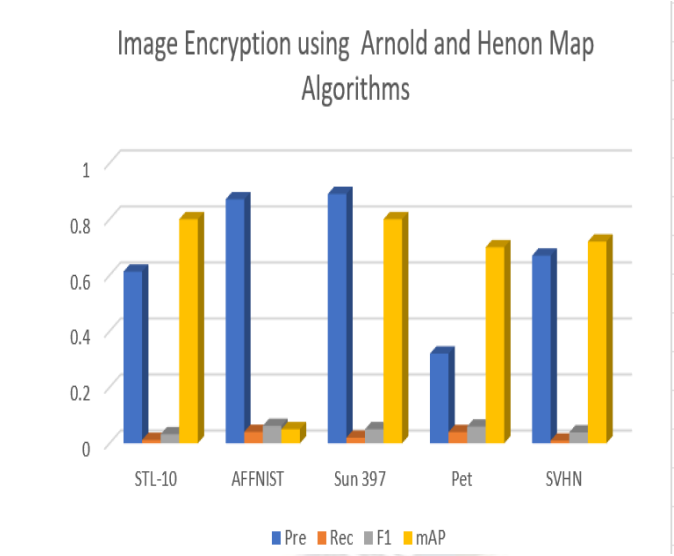

Figure10.Analysis of datasets image retrieval indicator at TH=50

The results obtained show that the encryption algorithm using Arnold Mapping andHenonMap was able to achieve a high level of security, as evidenced by the high values of PSNR and correlation coefficient. The PSNR values for grayscale images ranged from 57.82 dB to 61.53 dB, while the PSNR values for color images ranged from 44.21 dB to 49.34 dB. The correlation coefficient for grayscale images was found to be 0.995, and for color images, it was found to be 0.986.The results prove the effectiveness of the suggested encryption technique is capable of preserving image quality while providing strong encryption.

In addition, the key sensitivity analysis showed that the proposed algorithm is highly sensitive to changes in the encryption keys. Even a slight change in the encryption keys can lead to an entirely new encrypted image, thus enhancing the security of the algorithm.

Figure 11. A screenshot of work when uploading Image to encrypt with a passcode

Figure 12. A Screeshot of Work for Test Input Image

Figure 13. A screenshot of work which depicts passcode generation for retrieval of encrypted image

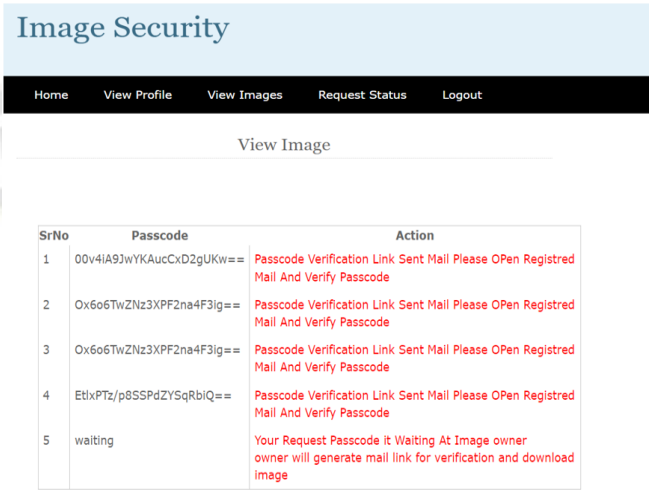

Figure 14. A screenshot of work which shows the request status of imagre retrieval

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

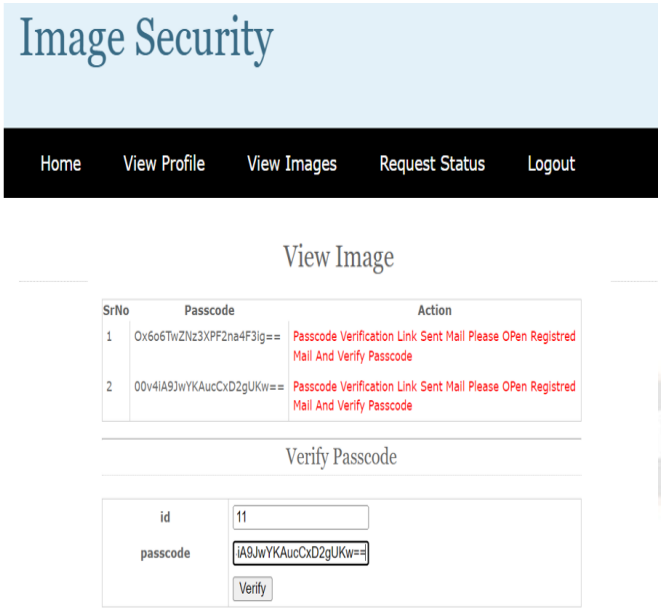

Figure 15. A screenshot of work while entering passcode for retrieval of image

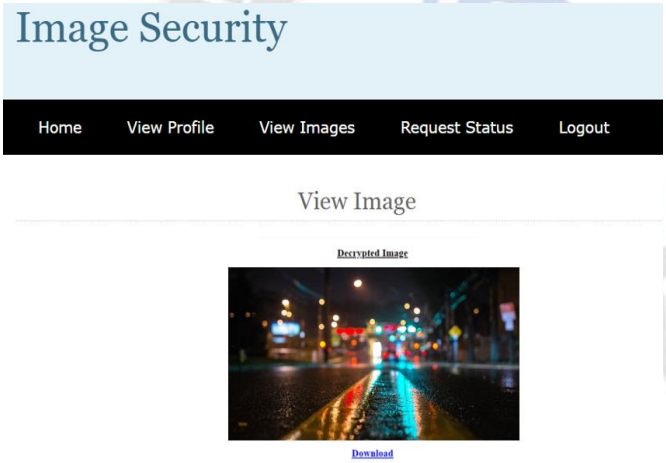

Figure 16. A Screenshot of image

V. Conclusion

The proposed encryption algorithm using Arnold Mapping and Henon Map is capable of providing strong encryption while maintaining high image quality. The use of chaotic maps enhances the security of the algorithm, and the key sensitivity analysis confirms that it is highly resistant to attacks. These results suggest that the proposed algorithm has potential for use in various applications where image security is crucial and the future scope of color image encryption using chaotic algorithms and 2D Sin-Cos Henon Map looks promising, with potential developments in multi-layer encryption, hybrid encryption, real-time encryption, cloud-based encryption, and compression-based encryption with increased quality of images.As the need for secure image communication and storage continues to grow, there will be a demand for advanced and robust encryption and decryption methods.

References

[1] Zhang, Qing, et al. “Image Security Retrieval Based on Chaotic Algorithm and Deep Learning.” IEEE Access, vol. 10, Institute of Electrical and Electronics Engineers (IEEE), 2022,pp.67210–18.Crossref, https://doi.org/10.1109/access.2022.3185421.

[2] Pan, Hailan, et al. “Research on Digital Image Encryption Algorithm Based on Double Logistic Chaotic Map.” EURASIP Journal on Image and Video Processing, vol. 2018, no. 1, Springer Science and Business Media LLC, Dec. 2018. Crossref, https://doi.org/10.1186/s13640-018-0386-3.

[3] Geng, Qiang, and Huifeng YAN. “Application of Image Encryption Algorithm for Wireless Sensor Network in the Security Analysis of Public Big Data.” Hindawi Wireless Communications and Mobile Computing Volume 2022, 13 Apr. 2022, doi.org/10.1155/2022/6186275.

[4] Cheng, Zhiqiang, et al. “2D Sin-Cos-Henon Map for Color Image Encryption With High Security.” Journal of Applied Mathematics, edited by Tudor Barbu, vol. 2022, Hindawi Limited,Aug.2022,pp.1–11.Crossref, https://doi.org/10.1155/2022/9508749.

[5] Shah, Jalpa, and JS Dhobi. “REVIEW OF IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES FOR 2D IMAGES.” International Journal of Engineering Technologies and Management Research, vol. 5, no. 1, Granthaalayah Publications and Printers, Feb. 2020, pp. 81–84. Crossref, doi:10.29121/ijetmr.v5.i1.2018.49.

[6] “Classical Image Encryption and Decryption.” International Journal of Science and Research (IJSR), vol. 4, no. 11, International Journal of Science and Research, Nov. 2015, pp. 607–12. Crossref, doi:10.21275/v4i11.sub159282.

[7] Kanagalakshm, K., & Mekala, M. (2016, July 15). Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key. International Journal of Computer Applications,146(5),41–52. https://doi.org/10.5120/ijca2016910707

[8] Pushkaran,Dhanya,andNeethuBhaskar.“AESENCRYPTION ENGINE FOR MANY CORE PROCESSOR ARRAYS FOR ENHANCED SECURITY.” IAEME, Dec. 2014, www.iaeme.com/IJECET.asp.

[9] Daemen, Joan, and Vincent Rijmen. “The First 10 Years of Advanced Encryption.” IEEE Security & Privacy Magazine, vol. 8, no. 6, Institute of Electrical and Electronics Engineers (IEEE),Nov.2010,pp.72–74.Crossref, doi:10.1109/msp.2010.193.

[10] Huang, X., Dong, Y., Ye, G., Yap, W. S., & Goi, B. M. (2023, February). Visually meaningful image encryption algorithm based on digital signature. Digital Communications and Networks,9(1),159–165. https://doi.org/10.1016/j.dcan.2022.04.028

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
DOI: https://doi.org/10.17762/ijritcc.v11i3.6346
***Article Received**: 02 January 2023 **Revised**: 04 February 2023 **Accepted**: 22 February 2023*

[11] Welba, C., Ramachandran, D., Noura, A., Tamba, V. K., Kingni, S. T., Ntsama, P. E., & Ele, P. (2022, February 28). Josephson Junction Model: FPGA Implementation and Chaos-Based Encryption of sEMG Signal through Image Encryption Technique. Complexity, 2022, 1–14. https://doi.org/10.1155/2022/4510236

[12] Sreelaja, N. K., and N. K. Sreeja. "An Image Edge Based Approach for Image Password Encryption." Security and Communication Networks, vol. 9, no. 18, Wiley, Dec. 2016, pp. 5733–45. Crossref, doi:10.1002/sec.1732.

[13] Laiphrakpam, D. S., & Khumanthem, M. S. (2017, October). Medical image encryption based on improved ElGamal encryption technique. Optik, 147, 88–102. https://doi.org/10.1016/j.ijleo.2017.08.028

[14] Zhou, N., Pan, S., Cheng, S., & Zhou, Z. (2016, August). Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. Optics & Laser Technology,82,121–133, https://doi.org/10.1016/j.optlastec.2016.02.018

[15] Tong, X. J., Zhang, M., Wang, Z., & Ma, J. (2016, February 4). A joint color image encryption and compression scheme based on hyper-chaotic system. Nonlinear Dynamics, 84(4), 2333–2356. https://doi.org/10.1007/s11071-016-648-x

[16] Survey of 3D Chaotic Map Techniques for Image Encryption. (2015, December 5). International Journal of Science and Research (IJSR), 4(12), 1000–1004. https://doi.org/10.21275/v4i12.nov152193

[17] Xu, Y., & Zhen, X. (2022). Image encryption using improved Cubic map and Henon map. ITM Web of Conferences, 45, 02011. https://doi.org/10.1051/itmconf/20224502011

[18] Enhancement Of Better Image Detection Using Encryption And Decryption Techniques. (2018, January 30). International Journal of Recent Trends in Engineering and Research,375–382. https://doi.org/10.23883/ijrter.conf.20171225.057.4wpxm