Image Encryption Using Henon Algorithm

Ms. Goli SumaLatha[*1], Mrs. P. Sri Jyothi[*2]

[1]MCA Student, Department of Master of Computer Applications,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.
[2]Assistant Professor, Department of Information Technology,
Vignan's Institute of Information Technology(A), Beside VSEZ,Duvvada,Vadlapudi Post,
Gajuwaka, Visakhapatnam-530049.
vignaniit.edu.in

Abstract:

A new evolutionary- grounded image encryption system is proposed to cover the image content against adversary attacks from an insecure network throughout the Internet. Two- dimensional Henon chaotic chart is the significant part of the encryption process, whereas its performance explosively depends on the fine tuning of its parameters, including α and β. Henon Algorithm is applied to determine these parameters grounded on the input simple image, so that the pseudorandom number generated by the two- dimensional Henon chart would be unique for each simple image, making it delicate to explore the encryption process. Experimental results assert that the proposed system is secure enough to repel against common attacks

Keywords: Two Dimensional,Encryption,Decryption,Adversary Attacks, Henon Algorithm.

1. INTRODUCTION

In the last many times, the security and integrity of the data is the most important concern. Now a day's nearly all the data is transferred over the computer networks, and it has increased the attacks over the network. Before transmitted data it must be translated and store so that it cannot be attacked by colorful bushwhackers. Encryption is a process of hiding the data, where it converts the original textbook into cipher textbook. Encryption uses different algorithm to cipher the data into different form. Cryptographic Algorithm uses a set of keys with the different characters for both encryption and decryption. By using key, the plain textbook is converted to the cipher textbook and decryption is done by converting back the plaintext from the cipher textbook. Cryptography is a process of transmitting and storing data in a form that it's read only by authorized druggies. Cryptography is a wisdom of protection of data by garbling it into undecipherable form. It's useful way of guarding the important sensitive information by using fine form algorithm for both encryption and decryption process. The encryption and decryption process depend on the crucial value. The strength of the algorithm is how delicate it's to determine the crucial value and get the original textbook. The algorithm is majorly divided into two types symmetric and asymmetric depending on the keys. However, also it's called symmetric algorithm, If same keys are used for both cracking and decoding. Symmetric algorithm is further divided into sluice and block ciphers. A sluice cipher is done on a single byte of data, whereas the block a cipher is done on the block of data. Asymmetric algorithm uses two different keys, one

for encryption and both for decryption. The key should be kept secret so that the communication shouldn't be deciphered. The purpose of cryptography is to give Authentication (proving the one's identity), non-repudiation (the receiver should know the sender shouldn't be faking), Integrity (data should be correct, delicacy, and responsibility), and sequestration/ confidentiality (communication is read by only the intended receiver).

2. LITERATURE SURVEY

[1] Title: Digital image encryption algorithm through unimodular matrix and logistic map using Python
Authors: Indra Bayu Muktyas; Sulistiawati; Samsul Arifin
Description: With the improvement of the communication speed and the popularization of the Internet, images have become the most common information medium in life. At the same time, the adverse effects of forged images in the media, credit investigation, finance and academic fields are becoming more and more significant. Therefore, in recent years, the research on forged image identification algorithms has been active worldwide. Image forgery has different classification methods. According to whether the forgery uses deep learning methods, it can be divided into deep forged images and traditional forged images. It can also be divided into ordinary image forged and document image forged according to whether the image is a text image. Different forgery methods will leave different forgery traces in the image, corresponding to different forgery identification methods. Aiming at document forgery images, this paper proposes a forgery detection algorithm based on deep learning and fusion of error level analysis (ELA) information. Compared with the previous forgery identification algorithms, the algorithm in this paper can not only identify whether the document image is forged, but can also locate the forged text area. The algorithm proposed in this paper supports the detection of document image forgery generated by cutting, copying, erasing and deep learning methods. The detection algorithm of this paper participated in the fifth forgery detection competition of Ali Tianchi and won the 32nd place among 1470 participating teams.

[2] Title: A novel image encryption algorithm using AES and visual cryptography
Authors:DPrabakar;R.Ganesan;D. LeelaRani;PraveenNeti.
Description:With the current emergence of the Internet, there is a need to securely transfer images between systems. In this context, we propose a secure image encryption algorithm that uses both AES and Visual Cryptographic techniques to protect the image. The image is encrypted using AES and an encoding schema has been proposed to convert the key into shares based on Visual Secret Sharing. The cryptanalysis of the algorithm is then performed and is proved to be secure. The proposed algorithm is then implemented using Python and the results are discussed along with the possible future modifications.

[3] Title: A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network

Communication
Authors: Noor Sattar Noor 1, Dalal Abdulmohsin Hammood.
Description: Sensitive information in the form of text, pictures, audio, and video are exchanged over communication systems. Cryptography is the application of techniques for encrypting data between the sender and receiver so that the receiver can read the data and an adversary cannot. Making sensitive data safe is critical with the overwhelming dependence on electronic communication systems in the modern world. Data may be transferred without the danger of being intercepted by employing several cryptographic procedures [1,2,3,4]. Encryption is the most common way to protect large amounts of text data [5]. Cryptography is a process to convert plain text into cipher using two types of key; symmetric and asymmetric key. Symmetric means that the same key is used between sender and receiver in encryption and decryption processes. The examples of symmetric keys are substitution, transposition, hill cipher, Play fair cipher, Vigener, and others. While asymmetric key means that there are two keys in encryption and decryption processing—a private and public key [6,7,8]. Figure 1 and Figure 2 illustrate the block diagram of the cryptography asymmetric and symmetric keys, respectively. Many approaches, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest–Shamir–Adleman (RSA), Triple Data Encryption Standard (3-DES) and other established procedures, are used to encrypt and decrypt data [9,10,11]. However, these approaches are still ineffective at encrypting large-scale text with high redundancy and large storage capacities. To alleviate these issues, researchers have developed various text-to-image encryption algorithms to increase text security and efficiency, thus improving robust cryptographic algorithms.

[4] Title: On deep learning approach in remote sensing data forgery detection
Authors: AndreyKuznetsov
Description: Digital image forgery is a known issue due to the increasing availability of technologies and software that make it easy to create distorted images. In order to counter such attacks, several approaches have been developed to detect fakes. Of particular importance are the methods for detecting distortions of a particular type of digital image - Earth remote sensing data, which can be used to ensure the safety of protected areas, monitor the state of the environment, etc. This article proposes a new scheme based on neural networks and deep learning, which is based on the use of the new convolutional neural network (CNN) architecture to improve the quality of detection of the most common type of attack on digital images - embedding duplicates. As part of the proposed architecture, additional preprocessing layers are used to improve detection quality. This approach also demonstrates invariance to distortions introduced into the duplicated region. Experiments show that the proposed solution exceeds the known copy-move detection algorithms - the metric value F1 reaches 0.77. At the same time the proposed deep learning approach shows high quality for the splicing detection task.

[5] Title: Image Forgery Detection Based on Parallel Convolutional Neural Networks
Authors:AhmetKorkmaz;CemalHanilçi

Description: As a result of the advancement of software tools used in digital image processing, it has become very easy to generate fake images by applying various manipulations techniques on the original (authentic) images. These manipulated images can easily be used with malicious intentions in important fields such as law, medicine and communication. Hence, image forgery detection, determining whether an image is original or forged, is an important task. In this study, an image forgery detection system is proposed by combining three deep neural network structures in parallel, unlike the uniform deep learning methods used in image forgery detection. The proposed method has been evaluated on three different datasets, and the results clearly demonstrate the efficiency of the proposed method with promising classification accuracy.

3. EXISTING SYSTEM

The variation in the characteristics of the multimedia data similar as correlation among the pixels and high redundancy of the image. thus, there were some limits where same ways cannot be used for protection all type of multimedia data. The traditional encryption algorithms may not use to encryption the image directly because of these reasons as the size of image will be not same as the textbook it may varies. Hence the traditional encryption algorithm may take longer time to cipher and decipher the image compare to text.

a. Computational time is high in exiting system.
b. High computing power is needed.
c. For networking Systems, it isn't effective.
d. Security is also a major issue

4. PROPOSED SYSTEM

The proposed system aims to establish a secure and reliable framework for storing and transmitting digital images, catering to applications such as multimedia systems, medical imaging, and military imaging systems. Given the increasing prevalence of the internet, cell phones, and multimedia technology, the focus is on addressing the critical issue of image security. The design proposes a secure image encryption and decryption mechanism utilizing the Henon algorithm.

Advantages of the Proposed System:

1. Enhanced Image Security:

- The use of the Henon algorithm ensures a robust level of security for digital images. Encryption and decryption processes are designed to be resistant to unauthorized access, providing a dependable means of safeguarding sensitive visual data.

2. Applicability in Daily Life Operations:

- The Henon algorithm, widely used in everyday technologies like smart cards, cell phones, automated teller machines (ATMs), and web servers,

brings a level of familiarity and trustworthiness to the proposed image encryption and decryption system.

3. Utilization of AES for Strong Encryption:

- The Advanced Encryption Standard (AES) is employed to encrypt the image in a different form using a key. AES is a well-established and widely recognized encryption standard, known for its strength and reliability in protecting data. It ensures that the encrypted image is secure and resistant to unauthorized decoding.

4. Verifiable Transformation:

- The cipher transformation applied to the image is designed to be verifiably different from the original plaintext. This ensures that unauthorized users cannot gain any insight into the original image, maintaining the confidentiality and integrity of the visual data.

5. Speed and Efficiency:

- The Henon algorithm is chosen for its exceptional speed compared to other block ciphers. Its design supports fast execution, making it suitable for real-time image encryption and decryption applications. The round transformation similarity further contributes to efficient processing.

6. Pipelining Compatibility:

- The system is designed to be compatible with pipelining, allowing for efficient data processing. This is particularly advantageous in scenarios where a continuous flow of images needs to be encrypted or decrypted in a streamlined manner.

7. Endian Neutrality:

- The absence of computation operations for the cipher eliminates biases towards big or little endian architectures. This ensures that the system can seamlessly operate in diverse computing environments without compatibility issues.

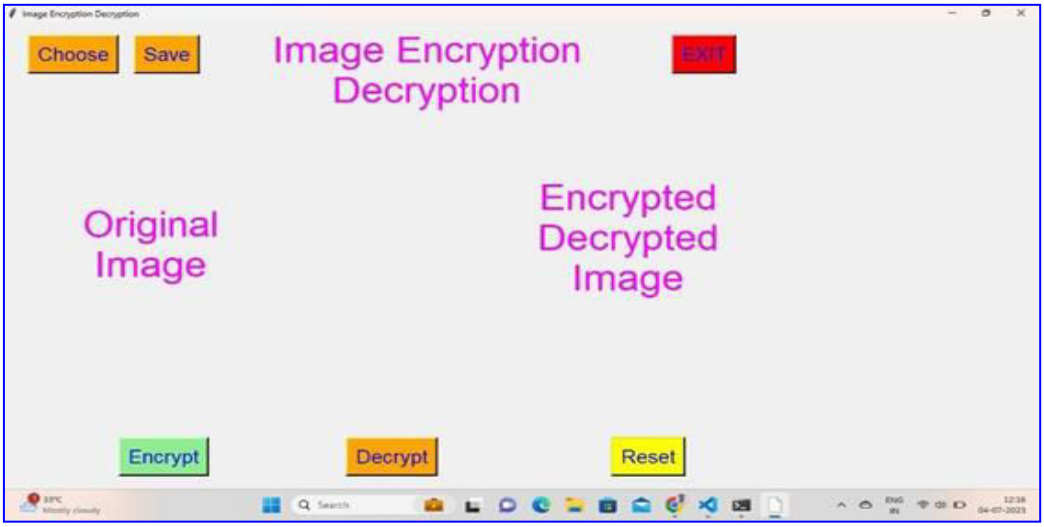
8. Transparency and Understanding:

- Unlike some encryption processes that rely on obscure or less understood methods, the use of AES in the proposed system provides transparency and a well-established foundation. This contributes to the system's reliability and ease of implementation.

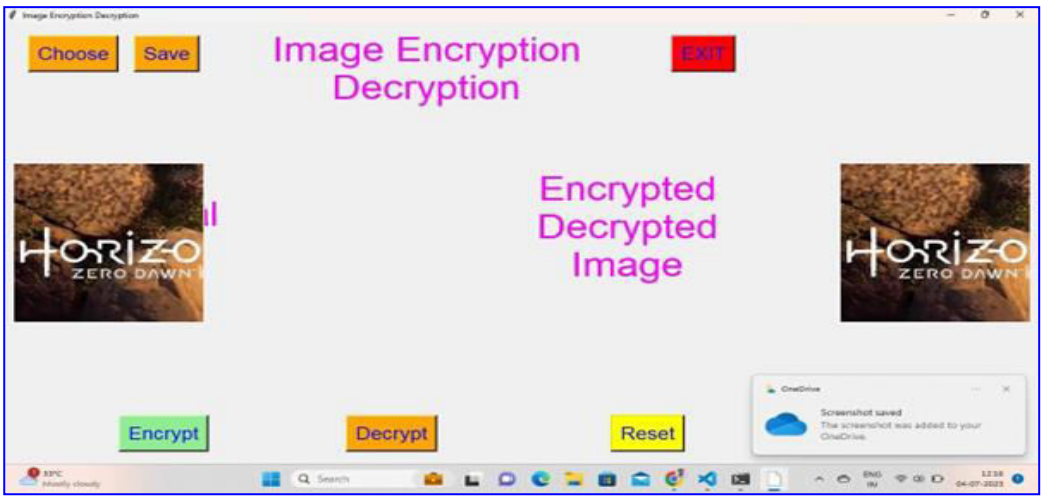
5. EXPERIMENTAL RESULTS

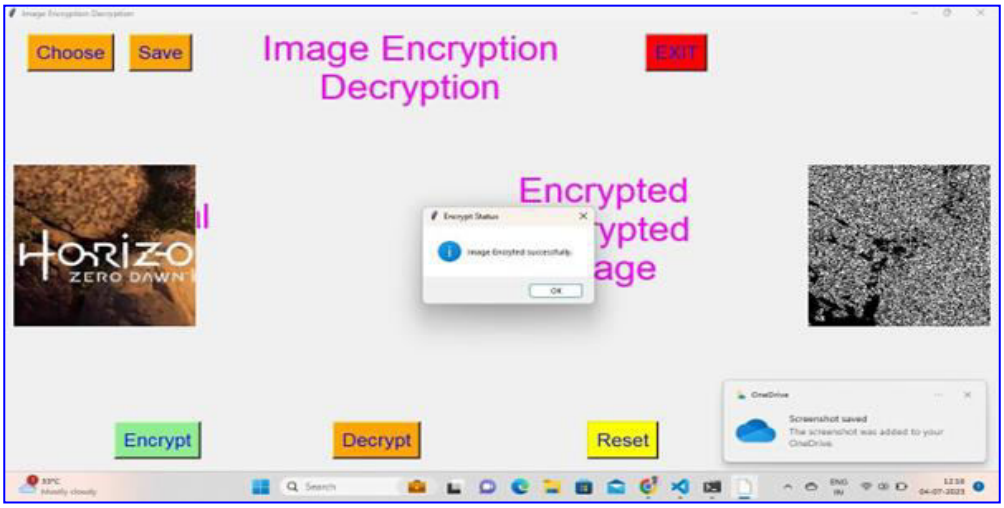
From the below figures it can be seen that proposed model is more accurate in order to prove our proposed system.

Main Window for Image Encryption and Decryption:

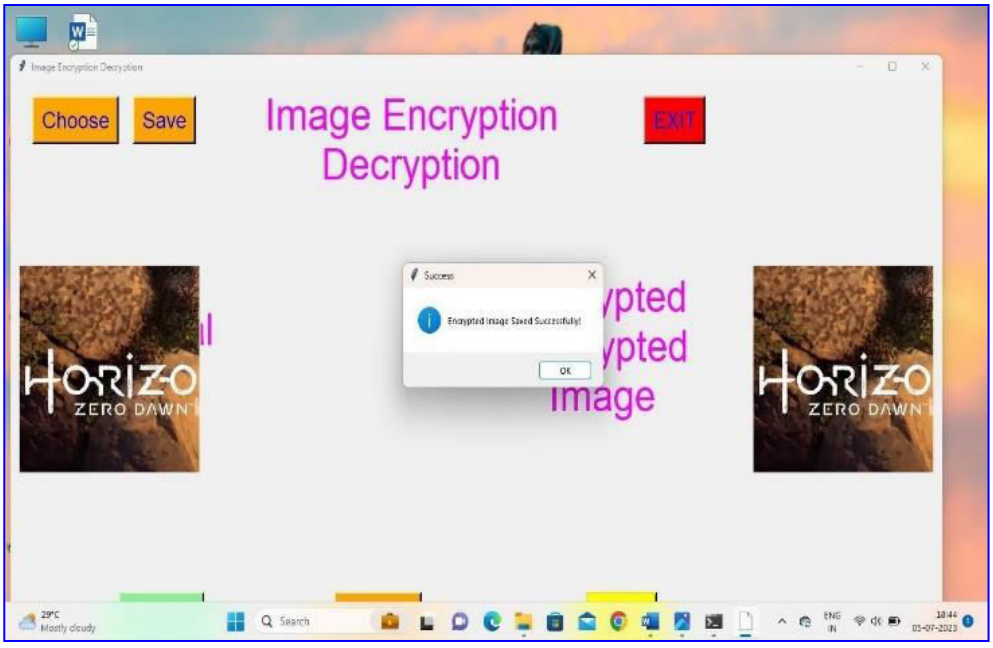

Choose
Save
Image Encryption
Decryption
EXIT
Original
Image
Encrypted
Decrypted
Image
Encrypt
Decrypt
Reset


tion
EXIT
Encrypted
Decrypted
Image
Encrypt
Decrypt
Reset


Choose
Save
Image Encryption
Decryption
EXIT
Encrypted
Decrypted
Image
Encrypt
Decrypt
Reset


Choose
Save
Image Encryption
Decryption
EXIT
Encrypted
Encrypt
Decrypt
Reset


Choose
Save
Image Encryption
Decryption
EXIT
Encrypted
Encrypt
Decrypt
Reset


Choose
Save
Image Encryption
Decryption
EXIT
Encrypted Image Saved Successfully!
OK

6. CONCLUSION

In conclusion, the Henon algorithm has shown promising results in the field of image encryption. It utilizes chaotic maps to generate pseudorandom sequences that are used to scramble the pixel values of an image, providing security and confidentiality. The key advantage of the Henon algorithm is its simplicity, as it only requires a few parameters to generate chaotic behaviour. Through various experimental studies, Henon image encryption has demonstrated good performance in terms of key sensitivity, resistance to statistical attacks, and robustness against various cryptographic attacks. It has shown potential in securing digital images for applications ranging from secure communication to content protection. However, despite its advantages, there is still a need for further research and development to improve the security and practicality of Henon image encryption. This includes conducting more comprehensive security analysis, exploring hybrid encryption approaches, optimizing performance, and strengthening the algorithm's resistance to advanced attacks. Overall, chaotic image encryption using the Henon algorithm holds great promise and offers unique advantages. With continued research and development, it has the potential to become a valuable tool in the field of multimedia security, providing enhanced privacy and protection for digital image.

References

[1]Mohammad Zakir Hossain Sarker and Md. Shafiul Parvez, “A Cost Effective Symmetric Key Crypto-graphic Algorithm for Small Amount of Data”, Proceedings of the 9th IEEE International Multi topic Conference, pp. 1-6, December 2005.

[2]Xun Yi Chik How Tan Chee Kheong Slew Rahman Syed, M., "Fast encryption for multimedia," IEEE Transactions on Consumer Electronics, vol. 47, no. 1, pp. 101-107, 2001.

[3]Yen J. C. and Guo J. I., “A new chaotic image encryption algorithm,” Proceeding of National Symposium on Telecommunications, pp. 358-362, December 1998.

[4]Jui-Cheng Yen and J. I. Guo, “A New Chaotic Mirror-Like Image Encryption Algorithm and its VLSI Archi-tecture”, Pattern Recognition and Image Analysis, vol.10, no.2, pp.236-247, 2000.

[5]Jui-Cheng Yen and J. I. Guo, “Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Re-alization”. IEEE Proceeding Vis. Image Signal Process, vol. 147, no. 2, pp. 167175,2000.

[6]W. Wang, J. Dong, and T. Tan, “A survey of passive image tampering detection,” in International Workshop on Digital Watermarking, pp. 308– 322, Springer, 2009.

[7]V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” IEEE Transactions on information forensics and security, vol. 7, no. 6, pp. 1841– 1854, 2012.

[8]Noor Sattar Noor 1, Dalal Abdul Mohsin Hammood.” A Fast Text-to-Image EncryptionDecryption Algorithm for Secure Network Communication”.

[9]DPrabakar;R. Ganesan;D. LeelaRani;PraveenNeti;”A novel image encryption algorithm using AES and visual cryptography”.

[10] Indra Bayu Muktyas; Sulistiawati; Samsul Arifin”Digital image encryption algorithm through unimodular matrix and logistic map using Python”.