IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

Visual Cryptography on Securing Image Data Using Machine Learning

Amreen Saba[1] and Dr. Raghavendra S. P.[2]
PG Student, Department of Master of Computer Applications[1]
Assistant Professor, Department of Master of Computer Applications[2]
Jawaharlal Nehru New College of Engineering, Shivamogga, India
amreensaba311@gmail.com and raghusp@jnnce.ac.in

Abstract: *With the rapid growth of the internet and the transmission channels, it has become easier for attackers to gain unauthorized access to visual information. Privacy considerations even affect academics collecting image collections for surveillance purposes. However, existing methods still risk being attacked. A system that takes information or images as an input, initial processing, and machine learning to give classification output has been designed to reduce this risk. An appropriate encryption procedure, like secret share creation or using different chaotic maps, is derived from this output, and used to secure the data. The decryption process is based on the encryption technique used, which helps to reconstruct the original data and allows for an evaluation of the accuracy and security level of the system. The goal of this technology is to increase the security of essential visual information by making the encrypted images harder for the attackers to decrypt. In the proposed work, various models are proposed and implemented. The result obtained is analyzed using PSNR and entropy.*

Keywords: Visual Cryptography, Encryption, Cryptography algorithms, Information hiding, Shamir's scheme, Visual secret sharing, Machine Learning

I. INTRODUCTION

Unauthorized people now have easier access to visual data thanks to the widespread usage of the internet and quick transmission methods. However, because cloud server owners have access to the database, it presents security risks to store photographs in outsourced storage because image leakage could result. Hackers may also target cloud servers with the intention of changing or disclosing picture contents. In this article, visual cryptography is suggested as a substitute for image encryption, which is a key technology for protecting private image content. For automatically identifying various security levels, a machine learning model is also recommended. A variety of encryption models are developed in the proposed study. Key sequences are composed of chaotic sequences. Following are the remaining sections: In section II, a literature survey is carried out. The proposed work is explained in section III. The result obtained is presented in section IV. The analysis of the results is carried out in section V. The conclusion of the proposed work is given in section VI.

II. RELATED WORK

Following a comprehensive literature survey, compiled a list of some of the most significant works.

Hong Chen and JustieSu-Tzu Juan [1] present an XOR-based Visual Cryptography Scheme (VCS) for grayscale and color secret images. The scheme encrypts the secret image into multiple shares using the XOR operation.

Huang, B.-Y.; Juan, J.S.-T. [2] presents on Flexible Meaningful Visual Multi-Secret Sharing Scheme by Random Grids. Multimed. Tools Appl.

Liu et al. [3] propose the encryption of real-time picture text using a pre-processing module in which CNN is transferred into Alex Net. They enhance encryption security by employing a pixel scrambling technique with a private key.

Masayuki Tanaka et al. [4] introduce a learnable image encryption scheme and verify it using a cipher dataset.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

P. Subba Rao [6] provides an overview of concepts and techniques in visual cryptography schemes, including secret image splitting, logical operations, and various constructions proposed by researchers.

Naor, Moni; Shamir, Adi (1995).[5] "Visual cryptography". Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science. Vol. 950. pp. 1–12. doi:10.1007/BFb0053419. ISBN 978-3-540-60176-0.

Naor and Shamir [7] suggest a (k, n) threshold visual cryptography strategy that divides a secret picture into n shadow images (shares), with k or more shares needed to visually recover the secret image.The mentioned studies contribute to a better understanding of visual encryption and information security in various applications, such as key management, message concealment, authorization, authentication, and entertainment [5,7].

Sifei Zheng et al. [8] propose a unique visual image encryption approach that encrypts the original picture into a visually meaningful masked image, providing both encryption and visual protection against attacks.

Tai-Wen Yue and Suchen Chiang [9] propose a neural-network strategy for visual authentication using visual cryptography, including user shares and a key share in the scheme.

Dipesh Vaya, Sarika Khandelwal, Teena Hadpawat [10] discuss the concept of visual cryptography, where a secret image is split into shares and combined to reveal the original image.

III. PROBLEM STATEMENT

The rapid expansion of the internet and the transmission channels simplifies unauthorized access to visual information. Storing images in delegated storage offers convenience and functionality, but safeguarding private image content becomes arduous due to security concerns.

The possessor of the cloud server has direct access to the database, increasing the likelihood of outsourced image leakage. Moreover, cloud servers are prone to breaches by malicious actors, potentially resulting in unauthorized disclosure and alteration of image data in the cloud. Image encryption emerges as a crucial technology capable of effectively safeguarding private image content. However, existing solutions still present a vulnerability to potential attacks.

IV. DESIGN AND IMPLEMENTATION

A Machine Learning classifier is employed to predict the cluster to which an image belongs. Based on the outcome of the classification, the encryption scheme is selected using either a visual encryption technique (secret-sharing technique) or chaotic maps for encryption. The choice of decryption technique, in turn, depends on the specific decryption method used to retrieve the original decoded image.

The various techniques used are adapted according to the decryption approach utilized, ensuring compatibility between the encryption and decryption processes.

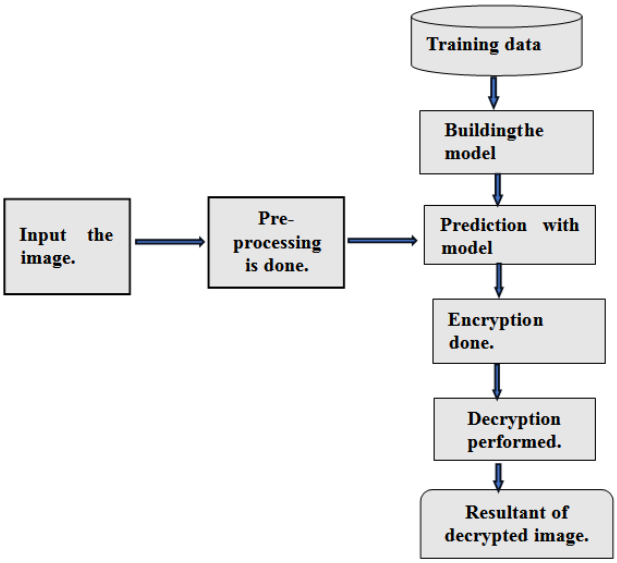


Fig.1 Proposed Design

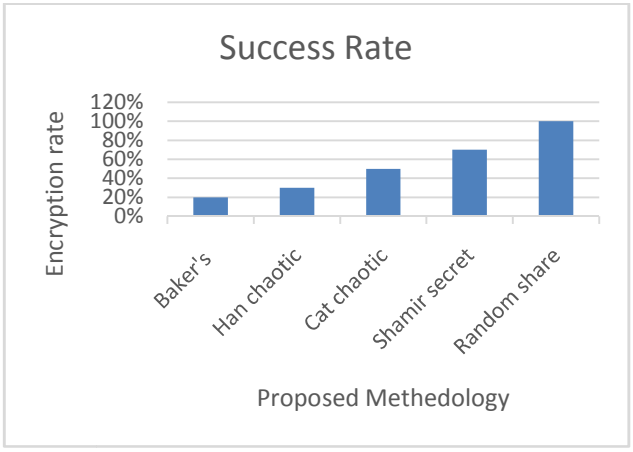
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

V. RESULT ANALYSIS

The results of the analysis are evaluated based on two metrics: peak signal-to-noise ratio (PSNR) and entropy [8, 9]. The experiments are conducted on a dedicated database consisting of 50 diverse images. The database includes multi-color images, uniform color images, as well as images containing text information. Table 1 presents the average entropy and PSNR values of the images in the database after applying encryption with various designed models. The table indicates that the Random share scheme demonstrates superior encryption performance compared to other techniques.

Table 1 Result Analysis

Designed Models	Entropy	PSNR
Shamir's Secret Sharing Scheme	7.6	9.12
Random Share Scheme	7.8	8.20
Baker's chaotic map encryption	7.43	10.01
Han chaotic map encryption	7.56	10.56
Cat chaotic map encryption	7.52	10.45



5.1 Results

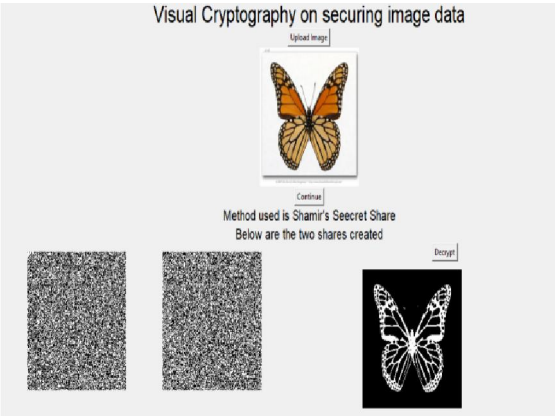


Fig. 2 Shamir's Secret Sharing Scheme

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

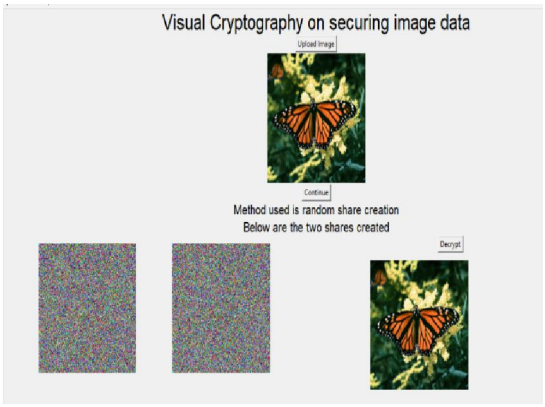


Fig. 3 Random Share Scheme

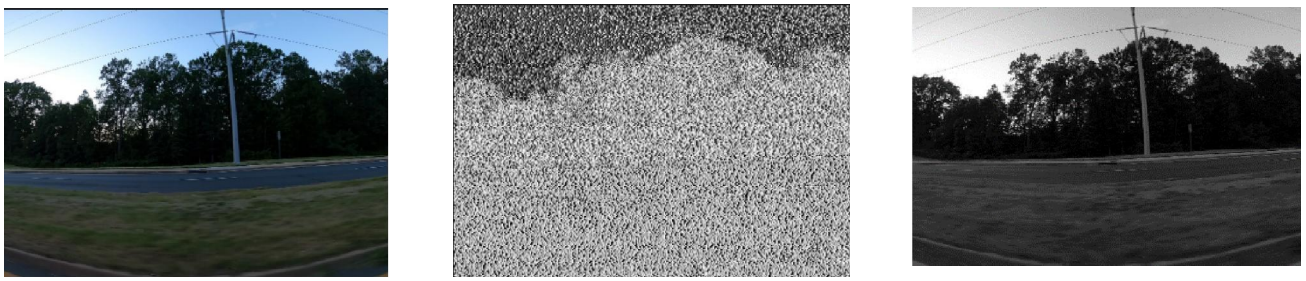


Fig 4 Baker's chaotic map encryption

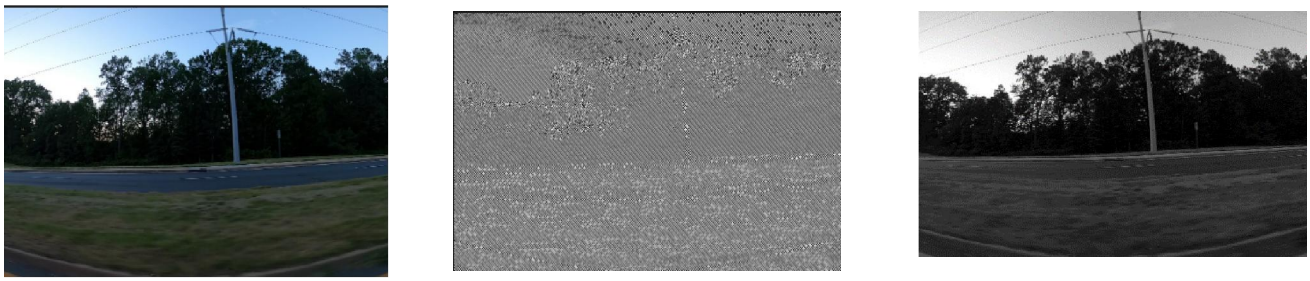


Fig 5 Han chaotic map encryption

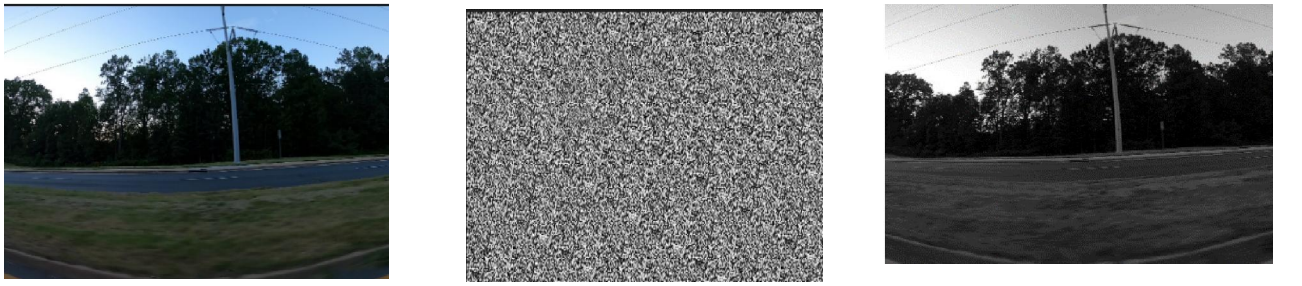
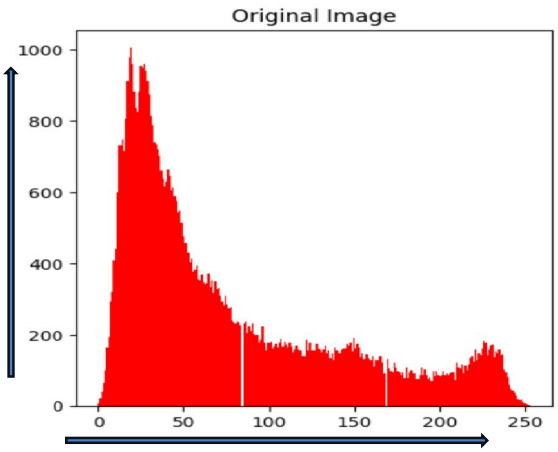


Fig 6 Cat chaotic map encryption

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

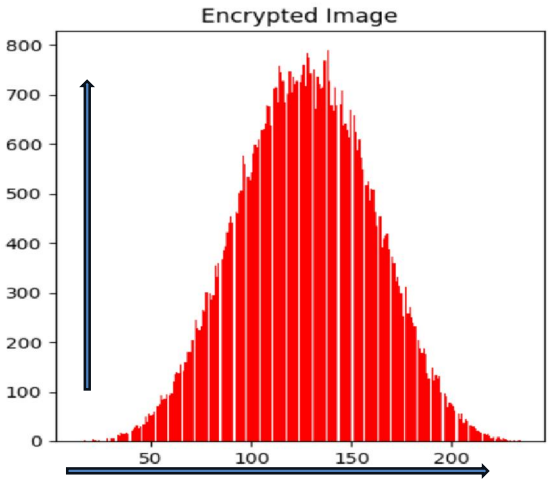
y-axis represents number of pixels.



x- axis represents intensity level.

Fig 7 Histogram of original image

y-axis represents number of pixels.



x- axis represents intensity level.

Fig 7 Histogram of encrypted image

VI. CONCLUSION

The development of the Internet has led to an increase in data breaches, as digital information is now accessible online. To mitigate these risks, various encryption and decryption techniques have been employed to safeguard sensitive data, including images. A recent study highlights the significance of integrating Visual Cryptography technology with machine learning for precise image classification. To achieve encrypted images, algorithms are utilized, and after classification, mapping to subsequent layers is performed. By employing appropriate algorithmic mapping, decryption becomes feasible. The proposed efforts will primarily concentrate on leveraging machine learning and visual cryptography to enhance the accuracy and security of data encryption.

REFERENCES

[1].Chen, T.; Tsao, K. Threshold visual secret sharing by random grids. J. Syst. Softw. 2011, 4, 1197–1208.
[2]. Huang, B.-Y.; Juan, J.S.-T. Flexible Meaningful Visual Multi-Secret Sharing Scheme by Random Grids. Multimed. Tools Appl. 2020, 79, 7705–7729.
[3]. Liang Liu et al.," Application of machine learning in intelligent encryption for digital information of real-time image text under big data", EURASIP J. Wireless Com Network (2022)2022-21

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, July 2023

[4].M. Tanaka, "Learnable Image Encryption," 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018, pp. 1-2, doi: 10.1109/ICCEChina.2018.8448772.
[5].Naor, M.,Visual cryptography. In: Advances in Cryptology - EURO-CRYPT'94, pp. 1–12. Springer Berlin Heidelberg (1995). DOI 10.1007/bfb0053419
[6]. P.Subbarao International Journal of Engineering Research & Technology (IJERT)Vol. 1 Issue 5, July – 2012 ISSN: 2278-0181.
[7].Shamir, "Visual cryptography," Advances in Cryptology EUROCRYPT'94, LNCS, vol.950, pp.1-10,1995
[8].Sifei Zheng et al.," Visual Image Encryption Scheme based on vector quantization and Content Transform", Multimedia Tools and Applications (2022) 81:12815-12832.
[9]. T. W. Yue and S. C. Chiang, "The General Neural-Network Paradigm for Visual Cryptograph," IWANN 2001, LNCS 2048, pp. 196-206, 2001.
[10].Vaya D. (2016) A Fast and Hardware-Efficient Visual Cryptography Scheme for Images. In: Advances in Intelligent Systems and Computing, vol 379, pp. 133-142, Springer, New Delhi.