Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Leveraging Noise Images for File Encryption

Reddyvari Venkateswara Reddy, Dude Srikanth, Phakirippagri Sumanth Reddy, Gatla Deepika
Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana State, India
UG Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana State, India

Abstract
In day-to-day life, there is a huge requirement for data transferring over the Internet, the data transfer between different entities may vary on the form of data and the level of encryption to keep the data secure and prevent it from any form of threat. There are different approaches to protecting the data and transferring it from one point to another over the internet keeping it safe. Sensitive information can be safeguarded from numerous risks by using cryptography. Enhanced cryptosystem technology is an obvious choice for network security. In the use of different cryptographic systems, our approach will work with any form of a cryptosystem by improving its efficiency to provide the added advantage of encryption and decryption of data using the uniqueness of randomness in the noise images. we are using a cryptographic system that generates noise images as a key which is used to encrypt the files and decrypt them later whenever required using the key.

Keywords **– encryption, decryption, noise image, Cryptography.**

I. INTRODUCTION

With data security playing the leading role in contemporary environment where corporate operations should be speeding up, defending sensitive information becomes a priority measure in cybersecurity. Surprisingly, 32% of the world business community permanently suffers from the pressure of hackers' bad actions and loses nearly $6 trillions annually. These organizations face a serious challenge of combating spam email by implementing high grade yet cost-effective solutions that is easy to integrate with their existing systems. Among them (security solutions), file encryption should be the cornerstone of well defense data protection plans (of organizations).

The file encryption covers not only the data protection but also the format of the file, whereby old information is encoded and any of it discloses through a vulnerable and insecure channel remain safe. The encryption here serves as an impenetrable wall against the malicious people, thus it blocks the unauthorized people to enter and change the data. An exclusive possession of obscured files by its intended recipient lock encouragement uses encryption as utmost security weapon for concealing confidentiality.

Data encoding through the usage of advanced algorithms helps to take the plain text and turn it into a distorted, meaningless set of characters. This transition which is irreversible is possible only those individuals who are in possession of the correct decryption key, usually the key are passwords or pass phrases. The majority of operations and surfaces offer encryption functionality, an in-house security mechanism that encrypts sensitive data in the dedicated areas which are only accessible via a decryption key. Cryptography, or the study of information encryption, that is used for this means usually takes secret keys (or terms of art the symmetric and asymmetric cryptography, respectively).

Public Key encryption- the even admiration diversified to different sectors operates with dual essential properties which are keeping and confidential. Such a way of encryption enables the message transmission from one party to another but without disclosure of the keys for decryption to anyone apart the one who has the private key.

Thus, while asymmetric cryptography uses two keys for generating successful transmission of information, the symmetric cryptography relies on a single key for both encrypting and decrypting messages. Therefore, it implies a secure key exchange between communicating devices. Traditional asymmetric encryption (such as RSA) is highly effective in simultaneously encrypting vast data sets while also maintaining data privacy during exchange for key management.

The right secrecy algorithm choice is very important. This includes such factors as the suitability of the specific system, effectiveness of the algorithm being used and the size of the key. There are diverse encryption standards used by different industries. However, this compatibility with various database content may also be slightly different in some cases.

Furthermore, more and more researches focus on the use of noise pictures as keys for image encryption and decryption, and

this suggests their potential applications at the high level of security due to the experiments that could verify them.

II. LITERATURE REVIEW

[1] This paper uses a design method based on cryptanalysis to make sure the encryption method is safe. The proposed method works with many types of image files and sizes (N M). The paper does a thorough study of the image based on its look, key space, energy, key sensitivity, contrast, entropy, homogeneity, histogram, correlation, UACI, NPCR, mean absolute error, chosen-plaintext attacks, noise and occlusion resistance, and encryption speed. numerical simulations and Visuals show that the method is secure and reliable.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

[2]For safe and effective transmission, the researchers suggested a technique for encrypting and compressing medical images. To decrease the file size and jumble the visual content, they combined the discrete cosine transform (DCT), arithmetic encoding, and chaotic sequence encryption techniques. With their approach, they were able to attain a high compression ratio and a decent PSNR.

[3] This text explains how to write messages in a hidden way using steganography, which comes from the Greek words for “hidden” and “writing”. There are different ways to hide important information in different types of files, and some are easier or harder than others. The LSB method puts the image of the hidden file in the smallest bits of the image that shows the file. You can use this method with 24-bit and 8-bit images. BPCS steganography puts secret data in the bit-planes of the image that shows the file. We replace every bit-plane that looks like noise with secret data, and the image quality does not get worse. This type of steganography is called “BPCS-Steganography”. We use AES, BPCS, and LSB steganography to hide the secret image in this study.

[4] The public-key encryption technique presented in this paper is based on features that can guarantee the security of file data and allow for flexible file sharing. This method is simple to use and implement, in contrast to the existing attribute-based encryption techniques that require a great deal of additional cryptographic data and are quite complex. The attribute private key is divided into two halves using this method: one for the user and one for the server. When a user has access to a file, the user and the server collaborate to utilize their respective portions of the attribute private key to decrypt the file.

[5] The scientists put out a technique for compressing and encrypting medical photos for safe and effective transmission. To minimize the file size and jumble the image content, they combined arithmetic encoding, chaotic sequence encryption, and discrete cosine transform (DCT). With this approach, they were able to obtain a strong peak signal-to-noise ratio (PSNR) and a high compression ratio.

Spatial domain

In spatial domain consecutively the pixel position and value within plain image are taken into consideration that cryptography process will be directly carried out on the certain pixel.

The function for image encryption can be expressed as follows:The function for image encryption can be expressed as follows:

$$E(x;y) = f[I(x:y)] \qquad \text{Eq.1.}$$

which means that 'Y' is a processed image in which (x, y) are coordinates of the plain picture, f is the processing function applied to the plain picture within the (x, y) neighborhood, producing (x, y) that are output coordinates of the encrypted picture.

In particular, the sum of Sfield and Ifield will give rise to an output field pattern, which is well recognized as the spatial domain. Pixels inside M number representation of the slope expressing any distance unit.

Frequency domain

The amplitude and phase shift components are the two basic features of a spectrum (frequency domain image), each of which frequency could be mathematically decomposed as series of frequencies. In other words, any differences in the spatial space will ultimately reflect in the space of frequencies. The frequency domain information is separated into two primary components: the level of noisy edges and your-finy-art pieces corresponds to the high-frequency component and the polished flat plane is the indicator of the low-frequency component.

Chaotic Image Encryption

So mathematics may also be one of them. A scheme is known by the name of a chaotic mathematical coded image encryption as an example. Being used with, this kind of ciphering makes pictures to transfer via any public broadcasting media and Internet channels almost indestructible. To bear in mind that, in the process of encrypting messages the cryptography specialists did a lot of efforts to produce the output random number generator which was both secure and effective. it was Edward Lorenz of the USA, who discovered the mystery behind chaos theory in 1969. Muks structures, mathematics, biology, engineering and philosophical physics as well as economics by 1970, it became established. Since there isn't a widely accepted definition of chaos in mathematics, a dynamical system can be considered chaotic if it possesses the following characteristics:Since there isn't a widely accepted definition of chaos in mathematics, a dynamical system can be considered chaotic if it possesses the following characteristics:

• It needs to be spatially mixed with others well.
• It should be very cautious when comes to start point and or inputs.

Topologically mixing is one of the properties of chaotic map ergodicity that allows to formulate that at certain finite numbers, all the orbits should pass through each of the regions of the state space if this state space is divided into regions. Even if the accounts are slighlty influenced by the initial conditions and control parameters, these variations should lead to outputs that differ greatly because of the sensitivity to these factors.

The area of cryptography is connected closely to chaos theory ever since 1990s in accordance with the observations announced by the researchers. Cryptosystems are supposed to take advantage of the finite world. On the other hand, for chaos, the continuous world is better.

This is the difference between the chaos of intercepting unencrypted traffic and the cryptography of eavesdropping on encrypted traffic. Nevertheless, the link between chaos cryptosystem and chaos is very strong, since chaos chaos is considered to have some properties like the sensitivity beginning conditions and mixing that resonate with the cryptography properties.

AI-Assisted Image Processing

Assessing the existing algorithms for Artificial Intelligence image processing is considered as a crucial task for the research team of many researchers. As, for one, the research [31] cited concerns machine learning combination with binocular stereo for depth estimation from images. The area of estimation of depths has many

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

really useful applications being divided into such domains as an estimation of depths at 3D reconstructions and autonomous driving. In the same techniques used for depth estimation, stereo matching of images that includes pixel disparity through triangulation to determining the depth of the pixel is an example. Advances in data-driven and learning-based approaches to stereo matching have been astonishingly fruitful and, vice versa, newly developed techniques applied to stereo matching long ago demonstrated the robustness of new methods working with deep networks.

The behavior of deep learning based MFIF arises as another major focus reviewed in work. MFIF is a subject matter that enables merging of numerous views together with perpendicular field of depth to form a picture which is perfectly in focus. It means that from 2017 on, the amount of papers which try to use deep training algorithms to solve this problem has risen substantially, but none of them have yet shown any kind of advantages or benefits over the formerly known method. Deep learning networks were the focus of another survey aiming at a better understanding of their role in picture segmentation. In various fields such as augmented reality, scene interpretation, video surveillance, and image compression, image segmentation has been found to be very useful. It is the dividing of an image into two or more segments. The performance of deep learning algorithms based on neural networks have shown incredible results in various cases where they have even beaten earlier segmentation solutions.

III. METHODOLOGIES

A. Backend Initialization

* The first step involves setting up a Django backend, which is a Python-based web framework. This backend will handle the business logic, data storage, and communication with clients.
* To initialize the backend, you'll typically start by creating a new Django project using the django-admin command-line tool. This sets up the basic structure of project.
* Within the project, we create one or more Django apps to organize your code. These apps can represent different components of your system, such as user management, file handling, authentication, etc.
* the backend is capable of processing and manipulating image data, as noise images will be used as keys for encryption.

B. Creating Algorithm (AES Encryption)

* The symmetric encryption algorithm is used for the purpose of reliable data security, with a set of different key sizes from 128 bits, 192 bits, or 256 bits.
* In Django, you can implement AES encryption by using libraries like PyCrypto or cryptography. These libraries provide functions for encrypting and decrypting data using AES.
* When encrypting data, you'll generate a random encryption key. This key is used to transform plaintext data into ciphertext, making it unreadable without the key. When decrypting, you'll use the same key to reverse the process and recover the original plaintext.
* the encryption algorithm will involve using noise images. These noise images can be generated using various techniques, such as random number generators, cryptographic hash functions applied to seeds, or even machine learning-based generative models.
* Each noise image serves as a unique key for encrypting a specific file. The randomness and complexity of the noise image enhance the security of the encryption process.
* When encrypting a file, you'll generate a noise image and use it as a key to perform bitwise XOR (exclusive OR) operation with the file data. This operation scrambles the file data using the pixel values of the noise image.
* Decryption involves applying the same noise image (key) to the encrypted file, effectively reversing the XOR operation and recovering the original file data.
* It's important to securely manage encryption keys, as they are crucial for protecting encrypted data. Django provides mechanisms for storing sensitive information like encryption keys securely, such as using environment variables or dedicated key management services.

C. Making a Table for the Database

* Django uses an Object-Relational Mapping (ORM) system to interact with databases. This allows you to define database tables using Python classes, known as Django models.
* In addition to storing user and file metadata in the database, you'll need to include fields to store information about the noise images used for encryption.
* Each encrypted file entry in the database would include a reference to the corresponding noise image key. This association ensures that the correct noise image is used for decryption.
* Depending on your specific requirements, you may also store additional metadata about the noise images, such as creation timestamp, owner information, etc..
* Once you've defined your models, you'll run Django's makemigrations and migrate commands to create corresponding database tables based on your models.

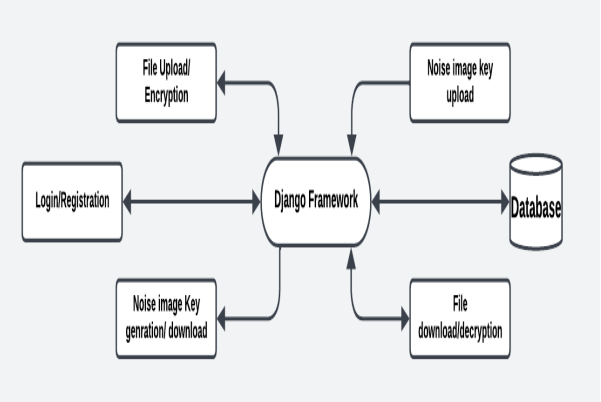

Fig.1: Flow diagram

IV. RESULTS AND DISCUSSION

The AES algorithm methods which are used in order to produce an outcome of a file after completing some steps in the encryption process as a result, be hashed and securely decrypted by the reliable software that is used for file storing. This strategy will ensure that the data is kept secure. The decryption revealed that the software can successfully encrypt binary files, as well as text files and any other type of file. These results demonstrate that the software is capable of providing a high level of file encryption

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

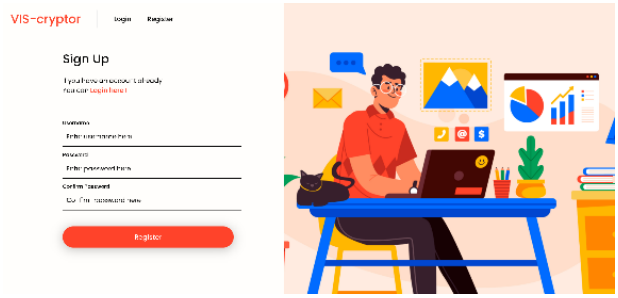

Fig.2 Login/registration page

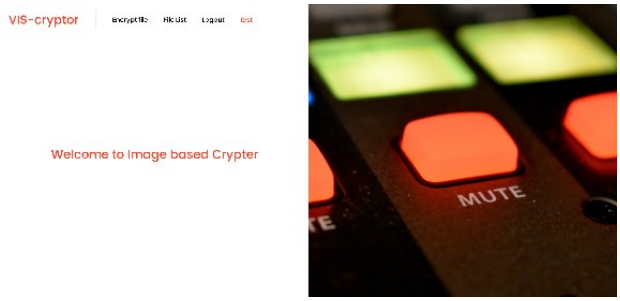

Fig.3 Home page

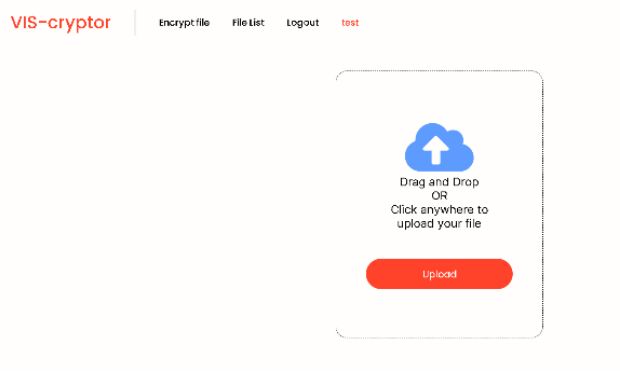

Fig.4 File Uploading

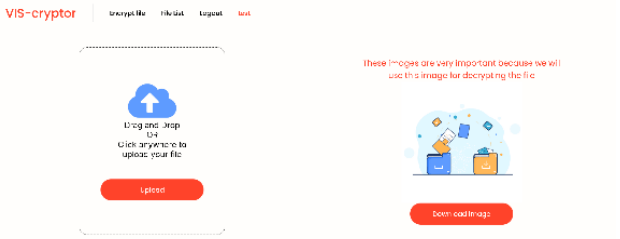

Fig.5 Noise Key image download

Fig.6 File List

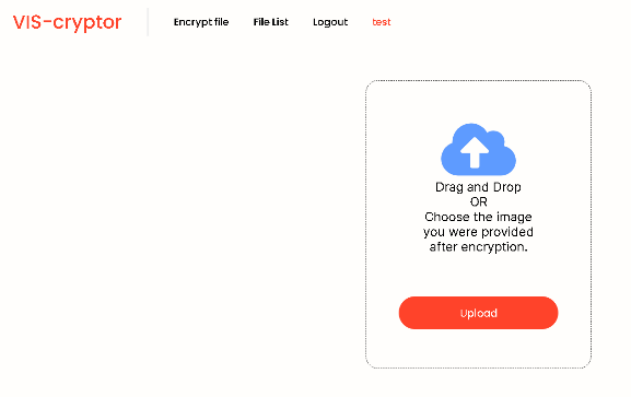

Fig.7 Noise Key Image upload for decryption

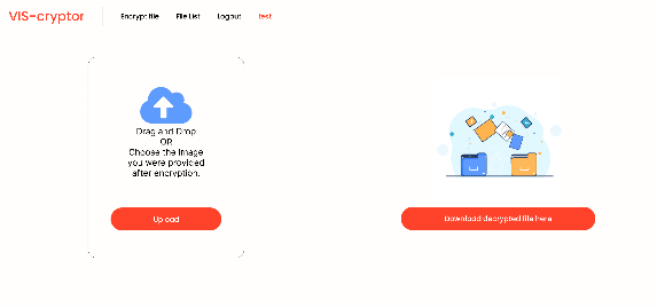

Fig.8 Decrypt and download file

Fig.9 image used for encryption.

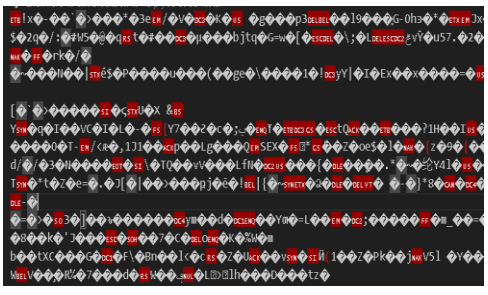

Fig.10 encrypted format of the above image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

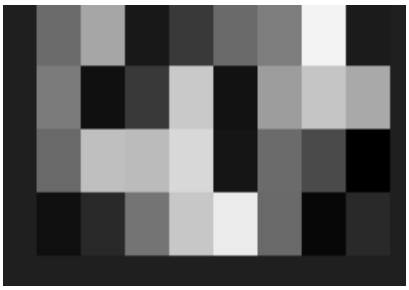

Fig.11 generated a unique key.

V. CONCLUSION

The file encryption is done with the help of algorithms of sufficient barrier. Thus, if the contents of the document has been shuffled by the method of encryption the document is referred as encrypted or garbled. In the case of garbled file, it is impossible to read, as you mention, however, whereas, the rascality of cyber-attacks comes in many forms and prejudices the information security as well. This piece of work was aimed at noise pictures as a primary method for file encryption, which allowed us to see its applications for several cases. Data from the examination project reveals the use of the given noise picture as the basic element in the encryption and decryption procedures being known as not only solid but also secure.

VI. REFERENCES

[1] B. L. A, P. R, S. K S and S. B, "File Encryption using Noise Images as Key," 2023 3rd International Conference on Smart Data Intelligence (ICSMDI), Trichy, India, 2023, pp. 206-210, doi: 10.1109/ICSMDI57622.2023.00046.

[2] M. D and S. Vasuhi, "Image Steganography: 2-Bit XOR Algorithm Used In YCbCr Color Model With Crypto-algorithm," 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2020

[3] J. Tong, Y. Long and Q. Liu, "A File Encryption System Based on Attribute Based Encryption," 2021 17th International Conference on Computational Intelligence and Security (CIS), 2021

[4] A. N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022

[5] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi and M. Samiullah, "A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes," in IEEE Access, 2022

[6] O. Q. J. Al-Thahab and A. A. Hussein, "Implementation of Stego-Watermarking Technique by Encryption Image Based on Turbo Code for Copyright Application," 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA), 2020

[7] P. Oktivasari, M. Agustin, R. E. M. Akbar, A. Kurniawan, A. R. Zain and F. A. Murad, "Analysis of ECG Image File Encryption using ECDH and AES-GCM Algorithm," 2022 7th International Workshop on Big Data and Information Security (IWBIS), 2022

[8] S. Patel and T. V, "New Image Encryption Algorithm based on Pixel Confusion-Diffusion using Hash Functions and Chaotic Map," 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022

[9] M. E. Kahla, M. Beggas, A. Laouid, M. Kara and M. AlShaikh, "Asymmetric Image Encryption Based on Twin Message Fusion," 2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP), 2021

[10] T. M. K. Afandi, D. H. Fandiantoro, Endroyono and I. K. E. Purnama, "Medical Images Compression and Encryption using DCT, Arithmetic Encoding and Chaos-Based Encryption," 2021 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2021

[11] C. Qin, J. Hu, F. Li, Z. Qian and X. Zhang, "JPEG Image Encryption with Adaptive DC Coefficient Prediction and RS Pair Permutation," in IEEE Transactions on Multimedia,2022

[12] S. Vasuhi and M. D, "Image Steganography: 2-Bit XOR Algorithm Used In YCbCr Color Model With Crypto-algorithm," 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2020

[13] J. Tong, Y. Long and Q. Liu, "A File Encryption System Based on Attribute Based Encryption," 2021 17th International Conference on Computational Intelligence and Security (CIS), 2021

[14] A. N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022

[15] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi and M. Samiullah, "A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes," in IEEE Access, 2022

[16] O. Q. J. Al-Thahab and A. A. Hussein, "Implementation of Stego-Watermarking Technique by Encryption Image Based on Turbo Code for Copyright Application," 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA), 2020

[17] P. Oktivasari, M. Agustin, R. E. M. Akbar, A. Kurniawan, A. R. Zain and F. A. Murad, "Analysis of ECG Image File Encryption using ECDH and AES-GCM Algorithm," 2022 7th International Workshop on Big Data and Information Security (IWBIS), 2022

[18] S. Patel and T. V, "New Image Encryption Algorithm based on Pixel Confusion-Diffusion using Hash Functions and Chaotic Map," 2022 7th International Conference on Communication and Electronics Systems (ICCES), 2022.

[19] M. E. Kahla, M. Beggas, A. Laouid, M. Kara and M. AlShaikh, "Asymmetric Image Encryption Based on Twin Message Fusion," 2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP), 2021.

[20] Poggi, M.; Tosi, F.; Batsos, K.; Mordohai, P.; Mattoccia, S. On the synergies between machine learning and binocular stereo for depth estimation from images: A survey. IEEE Trans. Pattern Anal. Mach. Intell.2021. [Google Scholar] [CrossRef]

[21] Zhang, X. Deep learning-based multi-focus image fusion: A survey and a comparative study. IEEE Trans. Pattern Anal. Mach. Intell.2021. [Google Scholar] [CrossRef]

[22] Minaee, S.; Boykov, Y.Y.; Porikli, F.; Plaza, A.J.; Kehtarnavaz, N.; Terzopoulos, D. Image segmentation using deep learning: A survey. IEEE Trans. Pattern Anal. Mach. Intell.2022, 44, 3523–3542. [Google Scholar] [CrossRef]]

[23] W. Dutta, S. Mitra and S. Kalaivani, "Audio encryption and decryption algorithm in image format for secured communication," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, India, 2017, pp. 517-521, doi: 10.1109/ICICI.2017.8365185.