Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024

STEGANOGRAPHY USING ADVANCED PARTITION ALGORITHM HADAMARD

Mrs. Prajwal Gailwad, Professor, Dept. Of Computer Engineering, AISSMS IOIT, Savitribai Phul PuneUniversity.
Mr. Jayesh Pawar, Student Of Computer Engineering, AISSMS IOIT, Savitribai Phule Pune University.
Mr. Arnav Amate, Student Of Computer Engineering, AISSMS IOIT, Savitribai Phule Pune University.
Ms. Pradnya Rajugade, Student Of Computer Engineering, AISSMS IOIT, Savitribai Phule Pune University.
Mr. Shreyas Todkar, Student Of Computer Engineering, AISSMS IOIT, Savitribai Phule Pune University.

Abstract
Data security has become crucial in era which is characterized by the rapid of explosion of various type ofdata transmitted through internet. When sensitive information travels over unsecure routes, it opens itself up to external threats like hacking. In response, a strengthened approach that combines steganography andcryptography has been adopted. The data is encrypted using techniques including LSB, DCT, DFT and hadamard transform; authentication is provided by a hash code produced by md5 hashing. Then, using steganography, the cipher text and hash code are hidden within pictures, sounds, or videos, adding an extra degree of protection. The Visual Secret Sharing Scheme (VSSS), which adds even more security, splits the media into several pieces so that any intercepted section only shows a portion of the text, making it useless to a hacker. This results in triple-layered security for safe data transfer since the recipient may reconstruct and decrypt the data upon receipt and validate it with the hash code. This
all-encompassing security plan helps to maintain data integrity and confidentiality by addressing the growing difficulties in protecting sensitive data in a time of growing data exchange and changing cyber-threats.

Keywords*:*
VSSS, Steganography.

I. INTRODUCTION

Cryptography involves encoding and decoding messages to protect sensitive information, with asymmetric and symmetric encryption algorithms being the main categories in contemporary frameworks.The purpose of the keys (public and private) in Secret-key encryption (SKE), commonly referred to as symmetric encryption algorithms (SEA), require a shared secret key between the sender and recipient for encryption and decryption. Public key encryption (PKE), sometimes referred to as asymmetric encryption, requires two keys from the sender and receiver; both a private and public key [1]. The symmetric algorithm has demonstrated its value, significance, and capacity to fulfill tasks and endure into the present day. upholding the goals of continuing message and data integrity and secrecy during transmission and when the data is at rest [2]. The method known as hash cryptography works without the usage of keys Instead, a fixed-length hash is computed using the plaintext value that, regardless of the plaintext's length or content, inhibits recovery [3].
The process of hiding sensitive information inside a file—which could be video, audio file, or image—isknown as steganography. [4]. The encoded data is implemented basic image using the LSB [5]. With thismethod, the LSB of the picture pixel value and the secret data to be concealed are subjected to an XOR operation. The least important portion of the basic image contains the result incorporated in it [5]. The overall change is so little that the humans are unable to detect the alteration in the base image. This algorithm is highly recommended because to its simplicity and minimal impact on degradation of

image quality [5].
Visual cryptography (VC) is a method where each participant owns shares to encrypt a secret image, preventing disclosure. It can be used to exchange and disperse secret images, including photographs, handwritten documents, and pictures. VC was initially designed for non-computer-assisted settings.

II. REVIEW OF LITERATURE

The main goal of this research [1] was to examine several approaches for integrating cryptography withsteganography to create a system that has capability of both cryptography and steganography.
Additionally, differences between steganographic and cryptographic techniques were discussed.
Three popular cryptographic algorithms are compared in this work [2]: one in asymmetric cryptography (RSA) and two in symmetric cryptography (DES, AES). In this, the underlying information and main cipher function of the algorithm under examination are easily understood. As a result, a summary of eachalgorithm's strengths and weaknesses is highlighted for examination.
This paper [3] proposes three hybrid encryption algorithms to safeguard data transfers: HMAC for symmetric password and/or data encryption, asymmetric RSA for AES password encryption, and symmetric AES algorithm for file encryption. To safeguard the encryption key or the data, Message Authentication Code, or MAC, is employed.
The use of elliptic curve encryption in an effective pairing-free CP-ABE access control technique for sharing information in poor application multimedia is described in this paper [4]. Only particular people who have been verified by the data owner are able to view the data. Users' resource and memory demandsare minimized when scalar product computations on elliptic curves replace pairing-based computations. By integrating crypto text into an image, the benefits of steganography and cryptography are combined to improve ownership, confidentiality, and security of information.
This research [5] employs the Hill algorithm with a hybrid elliptic-curve encryption technique. to encrypt text while minimizing processing overhead. After applying DCT to the hidden image, 40% of the DCT coefficients were incorporated into the original image. The DCT coefficients and the encrypted data were embedded into the picture using the LSB technique.
This paper [6] presents a watermarked color image algorithm according to the Singular Value Decomposition using Discrete Wavelet Transform (DWT-DCT-SVD) and Discrete Cosine Transform, andIt is necessary to first transform the color picture of the host from RGB to YUV. Next, the luminance component Y is subjected to the discrete wavelet transform.
The DCT is then used to divide the low-frequency component into individual blocks, and each block undergoes singular value decomposition (SVD). Place the watermark at the end of the cover image.
In order to protect 24-bit color pictures, this research [7] suggests a revolutionary method that employs steganography and cryptography. This method hides a picture inside another image using a randomized LSB-based technique. The final cover image is then encrypted using theory of chaos. This coordinated strategy ensures enhanced image security, a rise in data concealing capacity, and the unchanged retrieval of the concealed data. Additionally, it offers the idea of three levels of security: transmission via splitting, cryptography, and steganography.
This research [8] compares steganography methods for text and image encoding when a secret message needs to be hidden. In the field of steganography, various strategies are employed in this.
This study presents a revolutionary visual cryptography method using steganography to conceal the digital signature of hidden images. The method conceals secret bits in sharing blocks, modifies a white sub-pixel for binary 0, and can be recovered by comparing it with a rebuilt digital signature.
This work [10] presents a new encoding method that combines steganography with cryptography. Two layers of data encryption are used in the procedure, and the encrypted data is then hidden behind an image. The picture that contains the encrypted content is utilized for other objectives.
A hybrid cryptography technique that makes use of both the RSA and AES algorithms is used in this study [11]. To improve security, this hybrid cryptography encrypts the symmetric key that is used to encrypt messages as well. This paper's creation of a digital signature through message hash value

encryption is another noteworthy feature. The receiving end then uses this digital signature to confirm that the data is not change or hampered. The whole communication is then created by concatenating the encoded message, encoded symmetric key, and encoded digest. Again, the LSB steganography technique has been used to encrypt the entire message.
In paper [12], two degrees of data security are guaranteed by merging steganography and cryptography. With the use of the XOR operation and a user-selected key, a novel approach to data encryption and random embedding into an image representation is intended to be presented in this work.

III. PROPOSED METHODOLOGY

Using the AES and LSB algorithms, a novel method is presented in the suggested system to increase image security. We provide a strategy for (k, n) access structures by using the (k, k) sharing paradigm on each k-member subset based on specified relationships, given the susceptibility of an existing sharing technique to security breaches. As n increases, this strategy would need a significant amount of examples.Partitioning strategies are presented to cluster all the k-member subsets into multiple collections in order to solve this scalability problem. This makes it possible to swap out examples of several subgroups for a single representative. For the aim of the visual sharing schema, it is possible to conceal secrets within images using the suggested scheme. To effectively uncover the hidden secret, the private key needs to be in the possession of an authorized individual.

A. Advantages of designed system

Incorporates text that is both secure and effective.
2. Uses a unique partitioning method to increase security.
3. Makes sharing more effective.
4. Access structures that are highly flexible and secure.
5. There are less processing costs.
6. A hashing technique can be applied to confirm a message's correctness.

B. Architecture

The below fig. demonstrates the design of the suggested method:

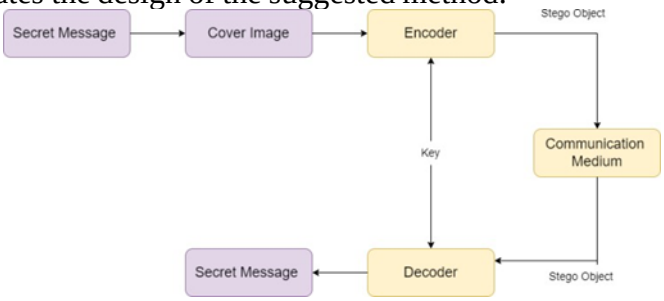


Figure 1. System Flow Diagram

C. Algorithms

1 Least Significant Bit Algorithm (LSB):

LSB is one technique used in steganography in the spatial realm. Data can be embedded into cover material or other kinds of data using the LSB approach. Images, sounds, or videos might be used as the cover media. Images with a bit depth of 8 or 24 can be used as a cover image to conceal hidden data. The image's most important data is carried by the MSBs of its pixels, while its least important data is carried by the Least Significant Bit. The necessary number of MSBs (Most Significant Bits) of secret informationcan be encoded behind the cover image's the LSBs (Least Significant Bits). As a result, the stego image that is produced by encoding the secret info into the cover image resembles the original. However, as more encoded bits of hidden info are present, the stego image and the Cover image become less similar [7]. Zero, for instance, is black. A value of 1 won't really change anything

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024
because the color is still black; it's simply a lighter tint.
The encoding process involves the action listed below:
1. Make the base image grayscale.
2. If needed, resize the image.
3. Transform the message into a binary file.
4. Start with an identical input and output image.
5. Perform the following operations by recursively going through each pixel in the image.

- Translate the value of each pixel into its binary representation.
- Obtain the subsequent portion of the message to be incorporated.
- Make the temperature changeable.
- Set temp = 1 if the LSB of the pixel and the message bit differ, and temp = 0 if they match.
- The value of {the temporary} can be determined simply performing an XOR operation between thepixel's LSB and the message bit.
- Modify the pixel value of the output picture so that it equals the sum of the input image's matching pixelvalue and the temp value.
- Until every bit of the message is incorporated, keep updating the output image.Save the input and output photos to the local system as a last step.

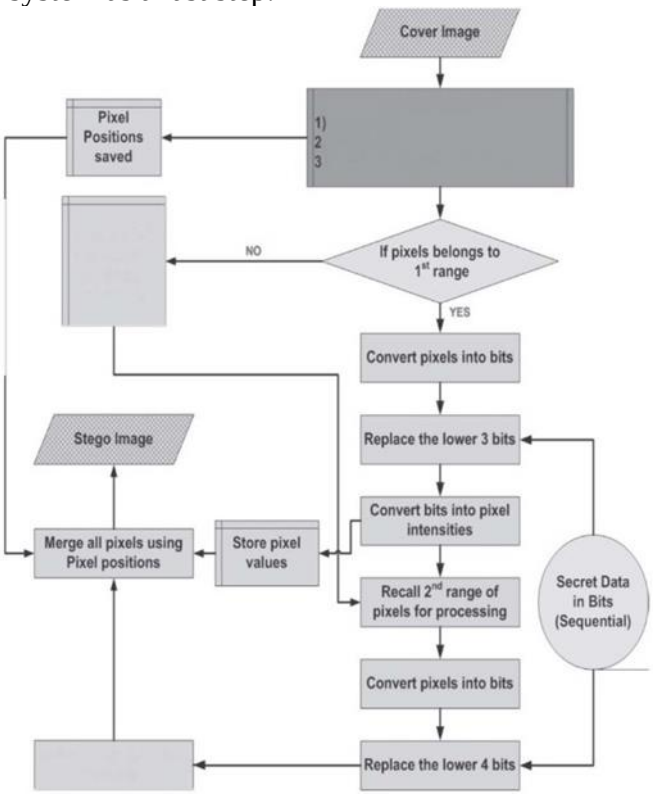


Figure 2. LSB Flow Diagram

In LSB steganography, the formula for embedding data into the lsb of a pixel's color channel (e.g., red, green, or blue) is:

\text { OldPixelValue +1} \ text {if DataBit = 1}\\ \text { OldPixelValue } \ text {if DataBit = 0} \end{ cases \ }

2.DCT

- DCT File compressor is responsible for taking images as input and com- presses them using DCT algorithm. We have used threshold factor of t = 0.2

The formula for DCT is a mathematical transformation used for image compression and

steganography. Itinvolves a summation over image pixel values and cosine functions. The formula for a 2D DCT is relatively complex and involves multiple nested summations.

– The forward equation, for image A is:

$$b(u,v) = \frac{2}{N} C(u)C(v) \sum_{X=0}^{N-1} \sum_{Y=0}^{N-1} a(x,y) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right)$$

–The inverse equation, for image B is:

$$a(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)b(u,v) \cos\left(\frac{\pi u(2x+1)}{2N}\right) \cos\left(\frac{\pi u(2y+1)}{2N}\right)$$

Here C(u)={$\frac{1}{\sqrt{2}}$ 1 $otherwise \ \ if \ u = 0$

3.DFT

In our system, we first determine the length of the secret message and then translate it into ASCII format. Next, we use DFT to apply equation (1) to change the cover image to frequency domain to spatial domain.Given that Fourier transforms are complicated and comprise both real and imaginary components, we only embed our secret data into the real portions of the transform. Once the secret information has been fully inserted, we use equation (2) to obtain the stego-image by performing Inverse DFT.

The image is represented using the DFT formula in frequency domain. It is the total of several complex exponentials, each of which represents a different frequency. For a 1D signal, the DFT formula is:

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi nk/N}$$

In the case of 2D DFT for images, you apply this formula separately to rows and columns.

4 Hadamard Transform

We will examine the Hadamard and Haar transforms in the next part. These transformations provide a significant computational benefit over the DFT, DCT, and DST transforms that we have already covered. They have unitary matrices that only contain ±1 values, and the transforms are calculated just byadditions and subtractions—multiplications are not necessary. This feature saves a lot of time, especially on CPUs that require a lot of resources to perform multiplication. Applying the Hadamard transform to data involves creating a square matrix called the Hadamard matrix, which has entries of ±1. The transform operation is essentially matrix multiplication. For an n-dimensional Hadamard matrix, the formula for the Hadamard Transform is:

$$H_n = \frac{1}{\sqrt{2}^n} \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

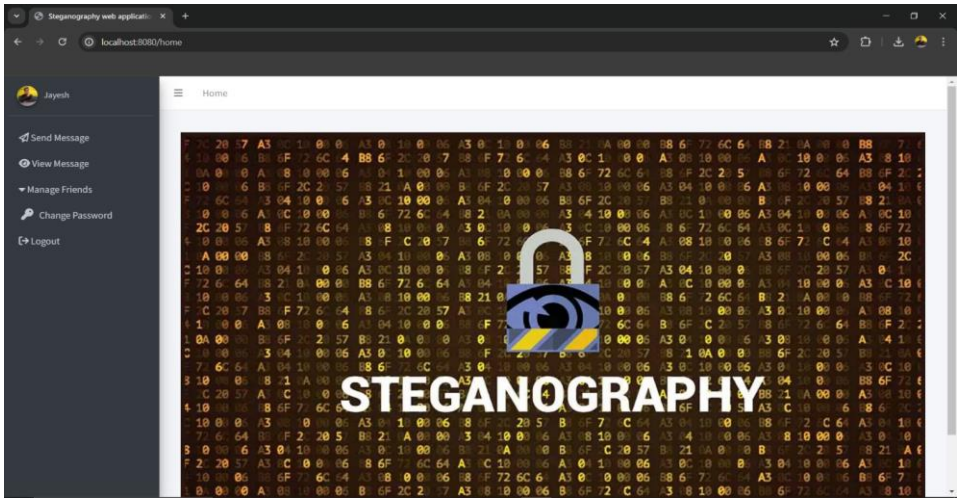
Where H_{n-1} represent the (n-1)-dimensional Hadamard matrix.

IV. RESULTS AND DISCUSSION

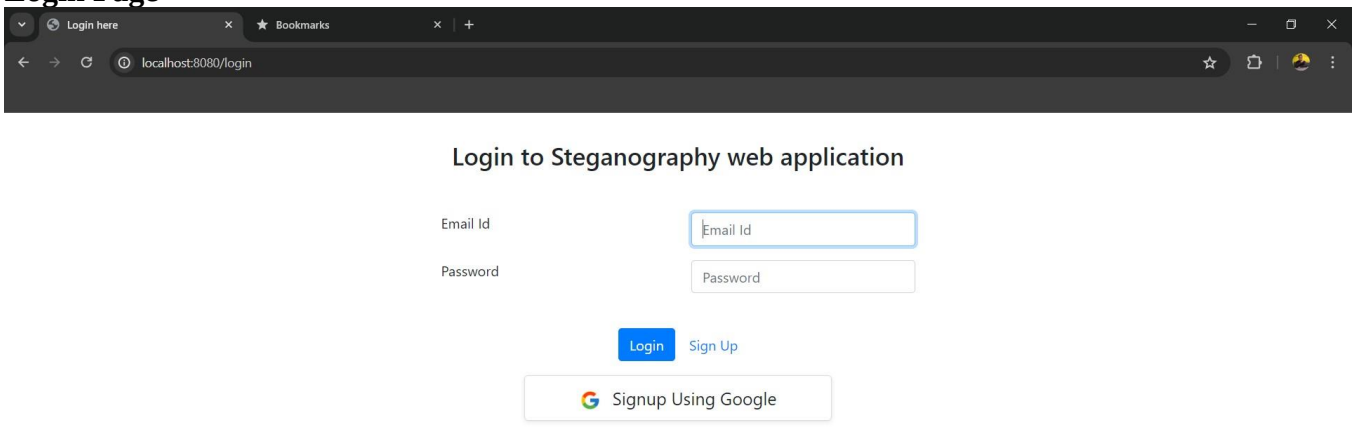
Personal computers equipped with the following specifications can be used for experiments: Windows, Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB RAM, Jdk 17, and MySQL as the backend database. The software was developed with Intellij tool kit and is a web program build in spring boot

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024

Home Page

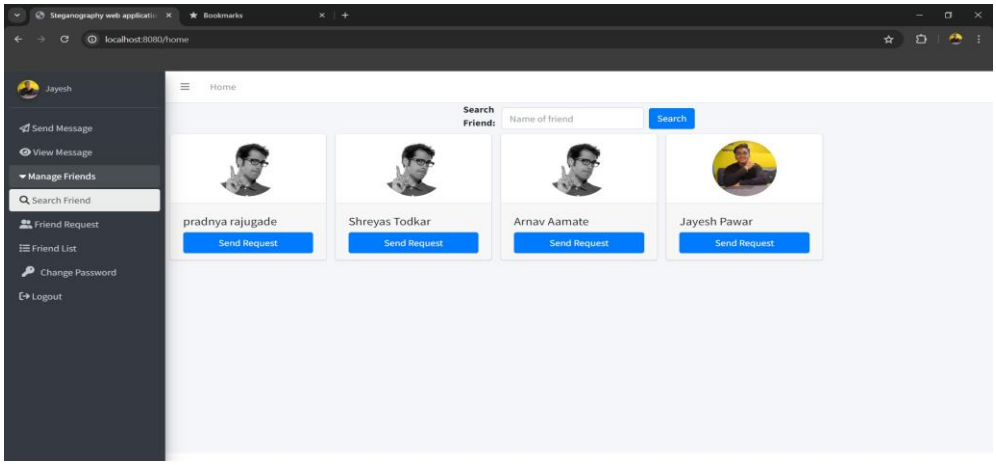


Login Page

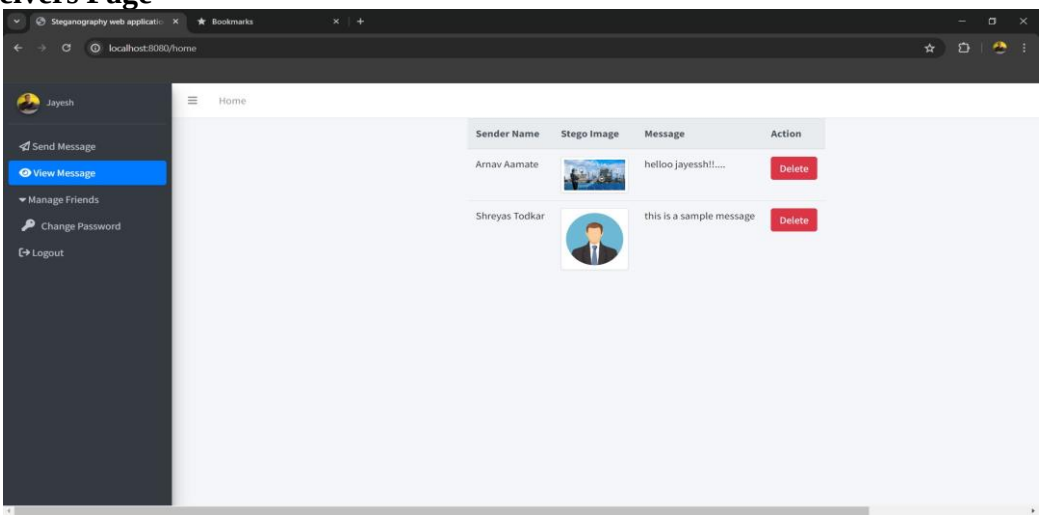


Search Receiver Page

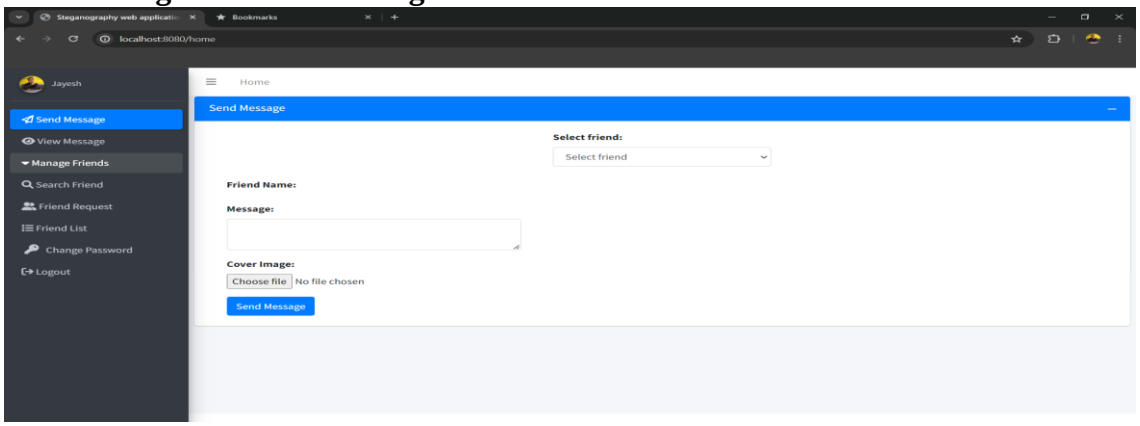
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024



View Receivers Page

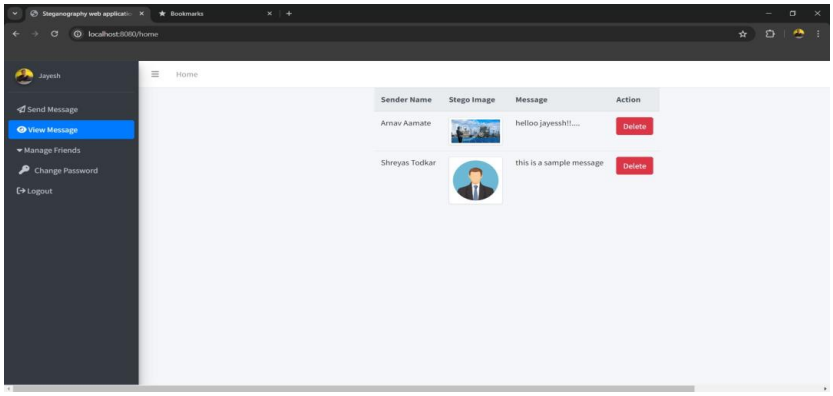


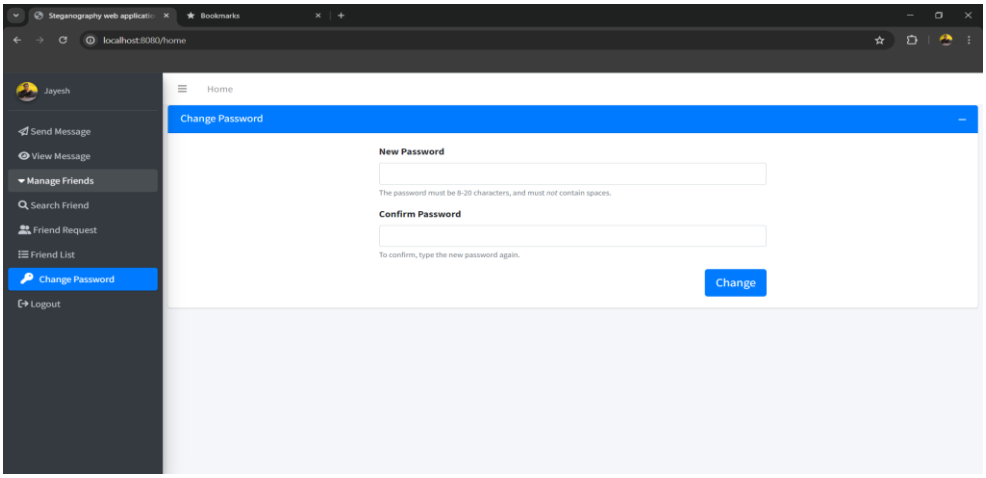
Send Secret Messages with cover image



Decode sender Message

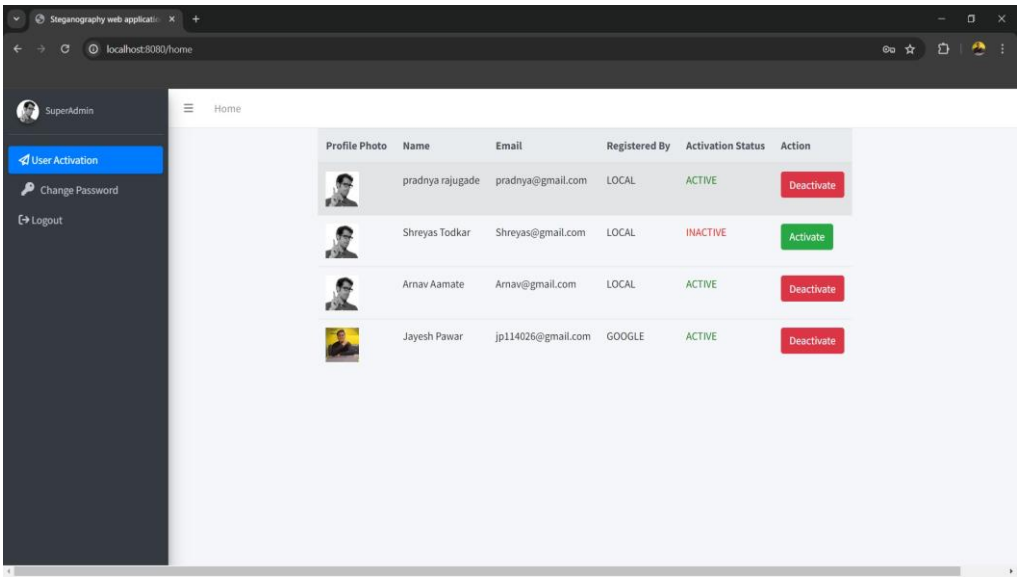
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024





Change_Password

Admin_Panal



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 4, No. 6, April : 2024

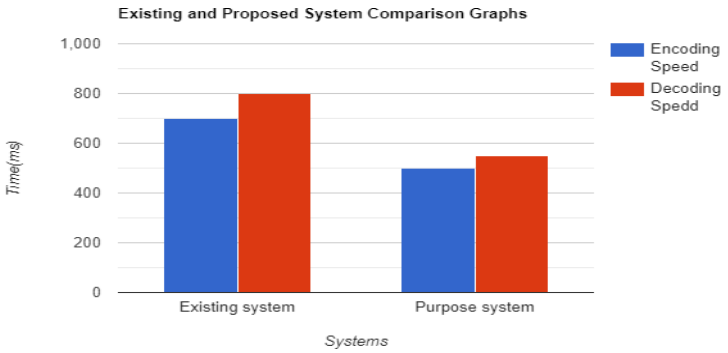


Figure 3. Existing and Proposed System Comparison Graphs

The time complexity of a sharing schema algorithm measures how much time algorithm requires to execute in comparison to the length of the input.

III. CONCLUSION

With the help of this research, we can protect our private data not only our personal private, but it can be also used to protect high profile secrets like government important records, company secret file. So, this project is as important to individual as much to public too. The system's encryption and decryption phases, coupled with secure transmission, provide a comprehensive security framework. While the project holds immense promise for safeguarding sensitive information, it does come with considerations such as algorithm complexity and resource requirements. Despite these limitations, the potential applications of this system are diverse and encompass secure communication in areas such as business, healthcare, government, and more. By addressing its limitations and adhering to legal and ethical standards, the project promises to be an asset in the realm of data security and privacy.

REFERENCES

[1] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).

[2] Aljaafari Hamza and Basant Kumar, "A Review Paper on DES, AES, RSA Encryption Standards", Proceedings of the SMART–2020, IEEE Conference ID: 50582 9th International Conference onSystem Modeling & Advancement in Research Trends, 4th– 5th, December, 2020 Faculty of Engineering & Computing Sciences.

[3] Eman Salim Ibrahim Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017.

[4] V. Reshma, S. Joseph Gladwin and C. Thiruvenkatesan, "Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications", International Conference on Communication and Signal Processing, April 4-6, 2019, India.

[5] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images", 2020 International Conference on Artificial Intelligenceand Signal Processing (AISP).

[6] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[7] Radha S. Phadte, Rachel Dhanaraj, "Enhanced Blend of Image Steganography and Cryptography," presented at the IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

[8] Khodher, M. A. A., & Khairi, T. W. A., "Review: A Comparison of Steganography Between

Texts and Images," presented at FISCAS 2020.
[9] Kh. Manglem Singh, Sukumar Nandi, S. Birendra Singh, L. Shyam Sundar Singh, "Stealth Steganography in Visual Cryptography for Halftone Images," presented at the International Conferenceon Computer and Communication Engineering 2008..
[10] Nidhi Menon, Vaithiyanathan V, “Triple Layer Data Hiding Mechanism using Cryptography and Steganography”, 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018), MAY 18th & 19th 2018.
[11] Biswas, C., Gupta, U. D., Haque, M. M., "An Efficient Algorithm for Confidentiality, Integrity, and Authentication Using Hybrid Cryptography and Steganography," presented at the 2019 International Conference on Electrical, Computer, and Communication Engineering (ECCE), February 7-9, 2019.
[12] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, “Secure Data Transfer Through Internet Using Cryptography and Image Steganography”, IEEE SoutheastCon 2020.