REVERSIBLE DATA HIDING WITH MULTIPLE SECRET SHARING USING CRYPTOGRAPHY APPROACH

DR.M DHURGADEVI

Associate professor

Department of Computer Science and Engineering

Mahendra Engineering College

SUSITHARAN R, SRINIVASH A, SETHUPATHY B, PRADHEESH S,

UG Students

Department of Computer Science and Engineering

Mahendra Engineering College.

ABSTRACT

Visual Cryptography (VC) is used to break an image into two random shares which when separately viewed reveals no information about the secret image. The secret image can be obtained by super imposing the two shares. Conventional visual cryptography scheme is used to encrypt a single image into n shares. The image can be decoded by using only shares. Many visual cryptographic methods use binary images only for this process. This doesn't suits well for many applications. First, the formulation of access structures for a single secret is transformed to that for multiple secrets. A sufficient condition to be satisfied by the encryption of MSS (Multiple Secret Sharing) schemes realizing an access structure for multiple secrets of the most general form is introduced, and two constructions of MSS schemes with encryption satisfying this condition are provided. Each of the two constructions has its advantage against the other; one is more general and can generate MSS schemes with strictly better contrast and pixel expansion than the other, while the other has a straightforward implementation.The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send secret information from the source to the destination in a secured way. The secret text was hidden within the image. The image is hidden inside an image using Modified LSB methodology. Then image is splited into shares and encrypted using XOR method. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images

simultaneously is achieved through this proposed work. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. At the receiver end, the hidden data is extracted from the recovered image. Experimental results show that the dimensions of the original image and the recovered image are same.

Keywords: Data Sharing Framework, Data Hiding, Multi Secret Sharing, Share Encryption, Key Sharing, Data Extraction.

1. INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous object (cover text) to produce a stego text. The recipient of a stego text can use his knowledge of the particular method of steganography employed to recover the hidden text from the stego text. The goal of steganography is to allow parties to converse covertly in such a way that an attacker cannot tell whether or not there is hidden meaning to their conversation. This sets steganography apart from cryptography which, although providing for private communication, can arouse suspicion based solely on the fact that it is being used.

Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text) with bits of different and invisible information. Hidden information can be any other regular computer file or encrypted data. Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message. Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is not seen.

1.1 DATA HIDING WITHIN IMAGE

Digital images are the most widely used cover objects for steganography. Due to the availability of various file formats for various applications the algorithm used for these formats differs accordingly.An image is collection of bytes (known as pixels for images) containing different light intensities in different areas of the image. When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color would be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded. Large amount of data can be encoded in to 24-bit images as it is compared to 8-bit images. The drawback of 24-bit digital images is their size

which is very high and this makes them suspicious our internet due to their heavy size when compared to 8-bit images. Depending on the type of message and type of the image different algorithms are used.

1.2MULTI SECRET SHARING

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Therefore the SS scheme is one of the most fundamental technologies to realize secure access control. A typical example of secret sharing schemes is a (k, n)-threshold secret sharing scheme. In (k, n)-threshold secret sharing schemes, a secret is encrypted into n shares in such a way that any k or more shares can be employed to reconstruct the secret, while no k − 1 or less shares leak any information about the secret. In the ordinary secret sharing schemes, secrets and shares are both numerical data and their encryption and decryption is performed by computers. In contrast, there exist secret sharing schemes whose decryption do not require any numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme is an example of such secret sharing schemes. In VSS schemes, secrets and shares are both visual data such as printed texts, hand written notes, pictures and so on. The schemes encrypt a visual secret into visual shares so that humans can recover the visual secret with their eyes by superposing a qualified set of visual shares printed on transparencies.

2. LITERATURE SURVEY

2.1 (SERVER-AIDED) TWO-PARTY MULTIPLICATION OF ENCRYPTED SHARES USING (K, N) THRESHOLD SECRET SHARING WITH N≥ K SERVERS

Kamal, et.al,proposed a method of multiplication by using only N ≥ k servers. This is implemented by sending two shares of the same input to each server. In a ‘‘normal’’ method, sending multiple shares to one server violates security because k shares can be leaked from k −1 servers. In our proposed distribution protocol, two encrypted shares for each secret input are sent to each server. In the typical Shamir’s (k, n) method, if multiple shares are distributed to one server, k shares are leaked from k − 1 servers (this immediately violates the security of (k, n) threshold secret sharing). For example, if the secret input a is distributed using Shamir’s (k, 2n) sharing (2n shares of input a are computed using a (k − 1) degree polynomial), and two shares are sent to each server, 2(k − 1) shares are leaked from k − 1 servers, and the adversary can reconstruct the secret input from these shares. Therefore, this approach violates the security requirement of (k, n) threshold secret sharing, where information from any k − 1 or fewer servers reveals nothing about the original secret input. In contrast, in our proposed method, multiplication is realized under the setting of n ≥ 2k − 1.

2.2 SEARCHABLE ENCRYPTION USING SECRET SHARING SCHEME THAT REALIZES DIRECT SEARCH OF

ENCRYPTED DOCUMENTS AND DISJUNCTIVE SEARCH OF MULTIPLE KEYWORDS

Ochiai, et.alimplemented a method that can realize the direct search function over sentences using the conjunctive search function without the construction of any index. Also propose a method that realizes the search function with multiple search queries using the disjunctive search function. Proposed model of secrecy computation is based on a client/ server model, where any number of clients (owner of the secret information) send shares of their inputs to multiple servers (n number of servers). However, clients who wish to search for any information (searcher) send shares of their trapdoors to n number of servers, which carry out the computation for the clients and return the results to them without learning anything. This model is widely used nowadays and is the business model. In proposed protocol, the searcher could produce valid trapdoor multiple times to perform searching. In addition, proposed methods assume a semi-honest adversary, where the adversary follows the protocol specification but may try to learn more than is allowed by the protocol, with at most k − 1 corrupted servers. In addition, also consider the following attacks: the adversary has information of the searcher in addition to information from k − 1 server and attempts to learn the registered document. Also presume that secure communication exists between the owner of the secret information, the searcher, and the servers. In the Proposed Method 1, by using the inverse computation of the logical conjunctive, we realized a total matching search function with multiple characters.

2.3 SECURE COMPUTATION BY SECRET SHARING USING INPUT ENCRYPTED WITH RANDOM NUMBER

Iwamura, et.al provided a secure computation with information-theoretic security against a semi-honest adversary is possible with $k \leq n < 2k - 1$. The TUS methods realize secure computation of secret sharing by using inputs that has been encrypted with random numbers. This is a combination of an encryption with a random number and computation using secret sharing. Proposed method is solved using the TUS 4 method, where the reconstruction of the multiplication result is only performed by the player that is allowed to know the result. It required when $n>k$. If the server or dealer distributes the random number using secret sharing to all n servers, even if $n-k$ servers are broken or lost, a substitute server can reconstruct the random number that was handled by the broken server and continue the computation. Thus, realizing the server loss resistance of secret sharing. However, it is important that the new server must handle the same random number as the server that it is substituting. This can be realized by implementing it in the algorithm (assuming a semi-honest adversary). Finally, it can be solved depending on the application considered. For example, when considering implementation in searchable encryption, because the owner of secret information will not be the adversary, it can be realized by requesting the

owner to generate random numbers that satisfy Condition.

2.4 A LIGHTWEIGHT PRIVACY-PRESERVING CNN FEATURE EXTRACTION FRAMEWORK FOR MOBILE SENSING

Huang, Kai, et.alproposed a novel lightweight framework for privacy-preserving CNN feature extraction for mobile sensing based on edge computing. To get the most out of the benefits of CNN with limited physical resources on the mobile sensors, design a series of secure interaction protocols and utilize two edge servers to collaboratively perform the CNN feature extraction. The proposed scheme allows us to significantly reduce the latency and the overhead of the end devices while preserving privacy. Several schemes have been proposed to outsource the tasks of CNN inference to the cloud servers. However, a deep CNN model typically has a substantially sophisticated structure that consists of many layers of non-linear feature extractors. The extra latency brought by the user-cloud and the inter-cloud interaction will become unacceptable since the users and the cloud servers are usually far away from each other. Moreover, to protect the privacy of the data, they usually utilize the computation-intensive cryptographic primitives like homomorphic encryption or garbled circuits.

2.5 PRIVACY-PRESERVING OBJECT DETECTION FOR MEDICAL IMAGES WITH FASTER R-CNN

Liu, et.alimplemented a lightweight privacy preserving Faster R-CNN framework (SecRCNN) for object detection in medical images. Faster R-CNN is one of the most outstanding deep learning models for object detection. Using SecRCNN, healthcare centers can efficiently complete privacy preserving computations of Faster R-CNN via the additive secret sharing technique and edge computing. To implement SecRCNN, here design a series of interactive protocols to perform the three stages of Faster R-CNN, namely feature map extraction, region proposal and regression and classification. To improve the efficiency of SecRCNN, we improve the existing secure computation sub-protocols involved in SecRCNN, including division, exponentiation and logarithm. The newly proposed sub-protocols can dramatically reduce the number of messages exchanged during the iterative approximation process based on the coordinate rotation digital computer algorithm. To reduce the communication overhead of the iterative approximation process, we redesigned the existing sub-protocols of common mathematical functions with the CORDIC algorithms. Then, we proposed a series of interactive protocols to implement the training and inference process of SecRCNN, which included feature extraction, region proposal, classification and bounding box regression. Based on SecRCNN, healthcare centers can collaborate to train a more accurate and more reliable model without concern of privacy disclosure.

3. EXISTING SYSTEM

RHD-EI allows a server to embed additional message into an encrypted image uploaded by the content owner, and guarantees that the original content can be losslessly recovered after decryption on the recipient side.

The proposed secret sharing based model with multiple data-hiders is comprised of three phases: the image encryption phase, the data hiding phase, and the data extraction and image recovery phase. Different from previous models that only involve single data hider, the proposed model involves multiple data-hiders. In the proposed model, the original image is converted into multiple encrypted images of the same size as the original image, and the encrypted images are distributed to multiple different data-hiders for data hiding. Each data-hider can independently embed data into the encrypted image to obtain the corresponding marked encrypted image. On the receiver side, the original image is reconstructed from a certain number of marked encrypted images, as well as the embedded data. In joint methods, data extraction cannot be performed in the encrypted domain. Marked encrypted images need to be decrypted with decryption key *kd* before data extraction, which indicates that the data extraction is related to the content-owner. In this scenario, the receiver needs to obtain permission from content-owner when verifying the integrity of the marked encrypted image. In separable methods, the embedded data is directly extracted from the marked encrypted image without decryption key *kd*, which indicates that the data extraction is independent of the content-owner. In this scenario, the data hider can update embedded data with a data hiding key as needed.

4. PROPOSED SYSTEM

The main objective of this project is to establish a secured communication between the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental security challenges of VC like external use of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares. The proposed method is n out of n multi secret sharing scheme. Transmission of multiple secret images simultaneously is achieved through this proposed work. Text message was created by sender and hidden within selected cover image file. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. The text is typed and hidden in an image. This is done using Modified LSB method. Then the XOR based VC method is used to encrypt the image and send it to the receiver. The key which is used to encrypt the shares will be mailed to the receiver. The receiver will decrypt the shares using the same key that is used for encryption. After that, the hidden text will be extracted from the recovered image using the Modified LSB method.

The proposed method provides secure communication between sender and receiver. In this method n out of n multi secret sharing scheme

was implementing to generate shares. Transmission of multiple secret images simultaneously is achieved through this proposed work. The secret text was present in the form of text files. That file will be created by sender to send at the receiver. The secret image can be revealed only when all the n shares are received by the receiver and decrypted. The text is typed and hidden in an image. This is done using Modified LSB method. Then the XOR based VC method is used to encrypt the image and send it to the receiver. The key which is used to encrypt the shares will be mailed to the receiver. The receiver will decrypt the shares using the same key that is used for encryption. After that, the hidden text will be extracted from the recovered image using the Modified LSB method.

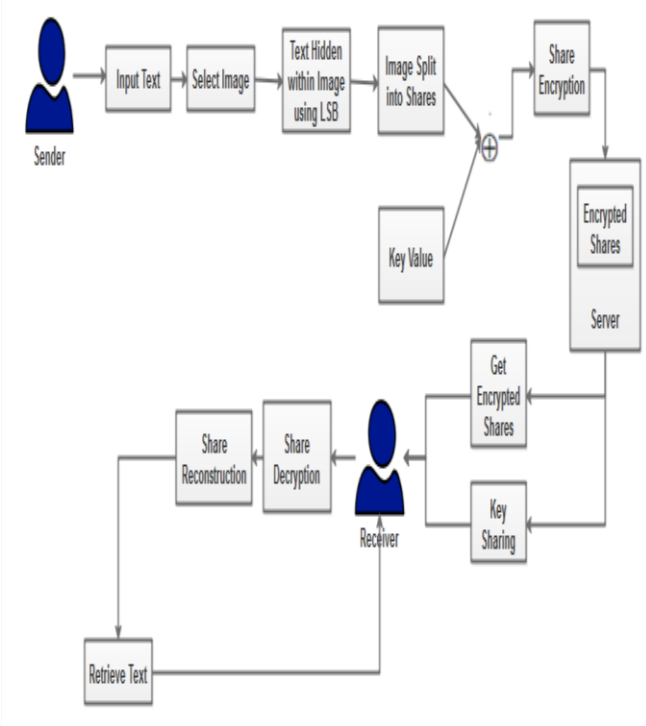
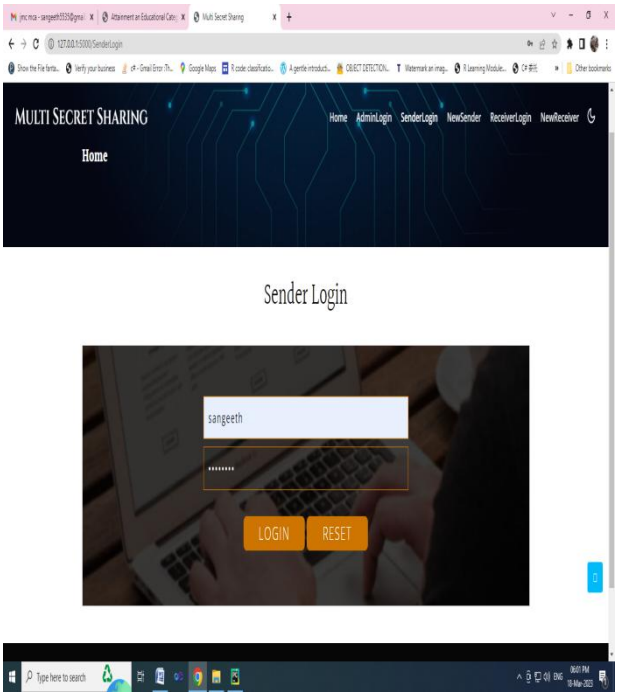


Fig 4.1: Architecture for Proposed Work

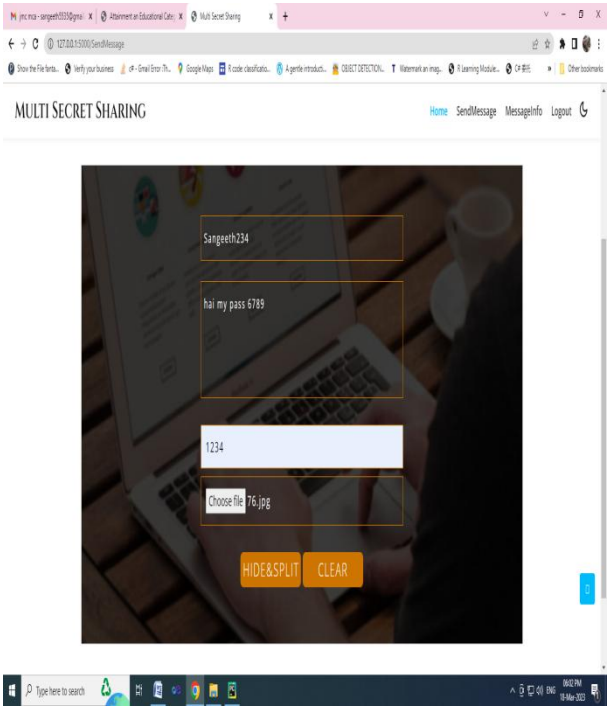
4. EXPERIMENTAL RESULTS

This proposed multi secret sharing system was implemented using Python as front end and MySQL as back end software. The implementation results shown below,

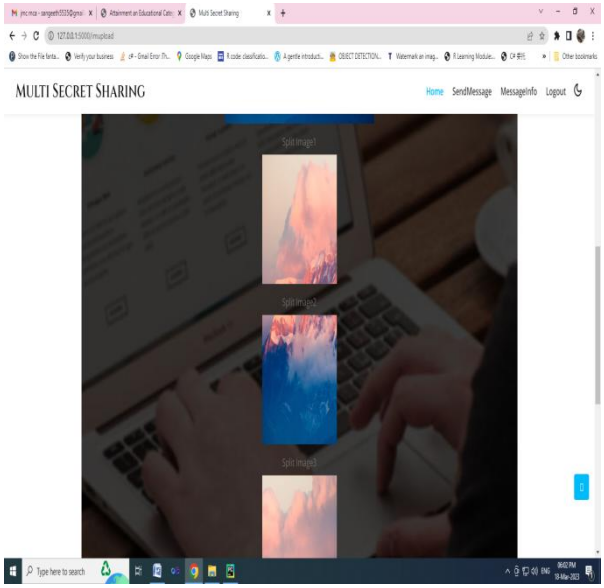
Sender login



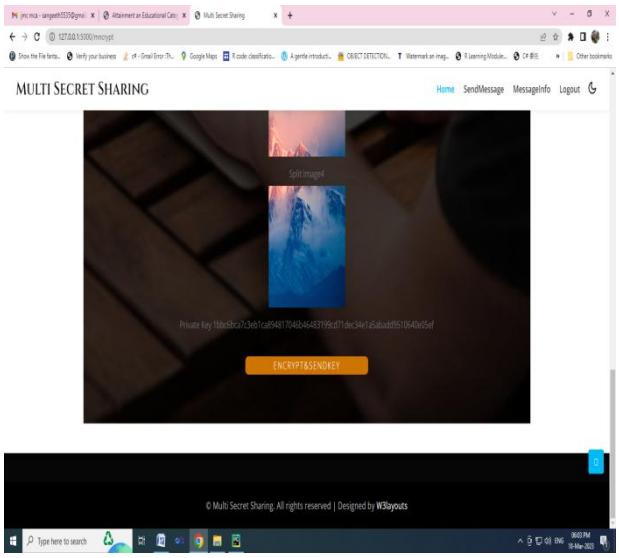
Input Text and Image



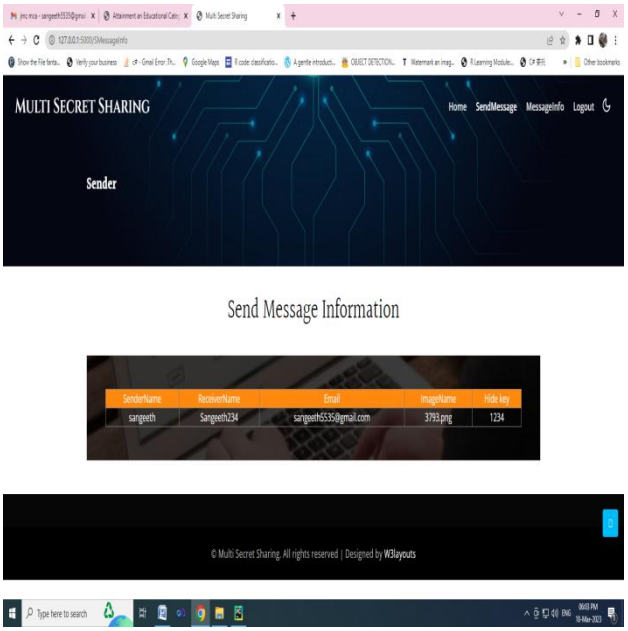
Multi Secret Sharing



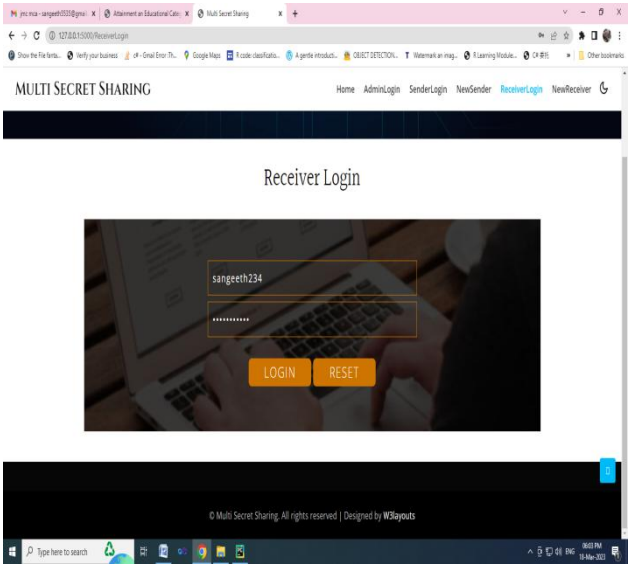
Share Encryption and Send



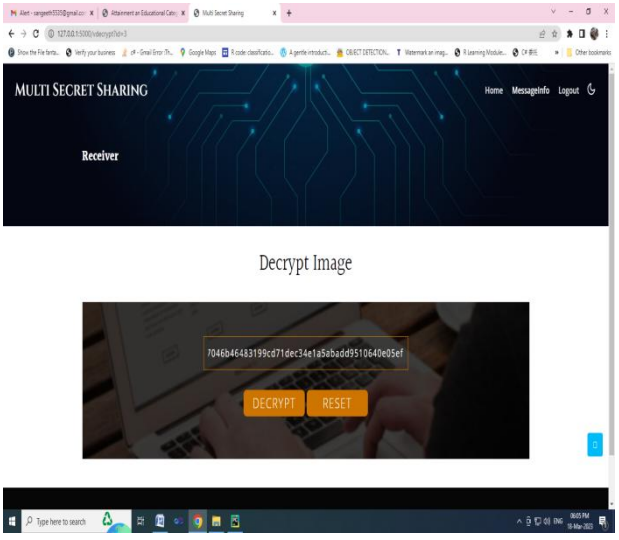
Send Details



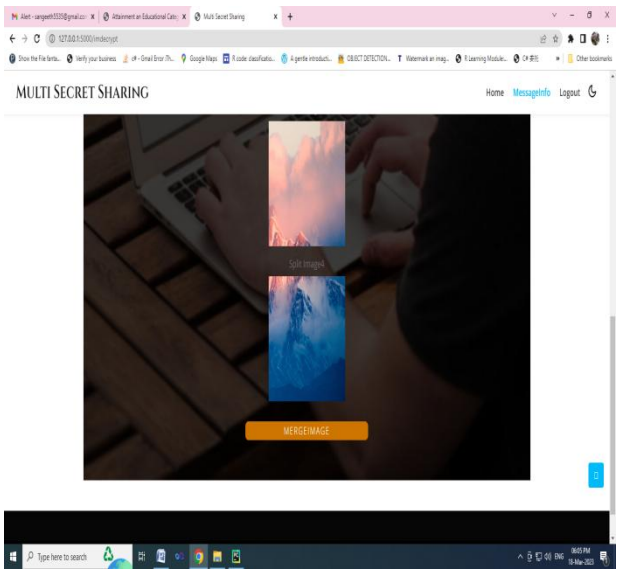
Receiver Login



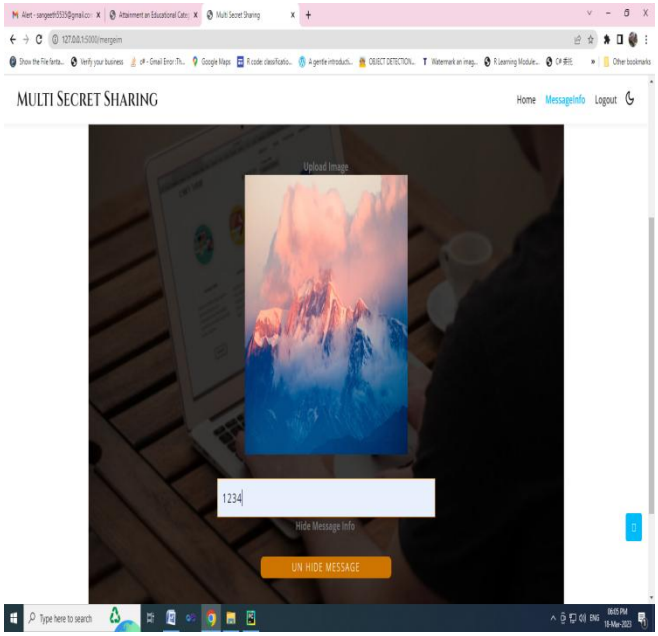
Decrypt Shares



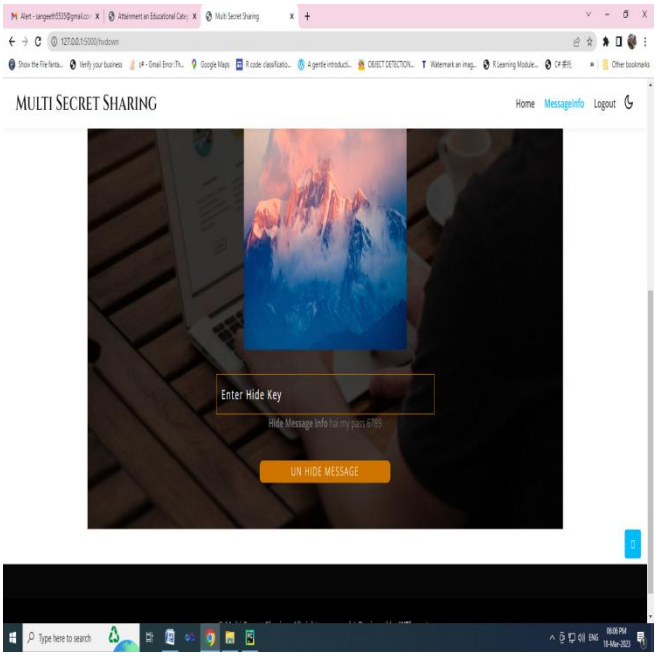
Decrypted shares



Data Extraction Key Verification



View Secret Data



5. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. The sender has to select the image that should be sent secretly to the receiver. The secret image is splited into “n” number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.The confirmation, outfitted with the thought behind the strategy guarantees that an enemy can't alter the last picture without messing with the previous, which makes its security analysis less difficult and more pragmatic**.**Itwill bethe subject of future work to explore the validation in more detail.

6. REFERENCES

[1] Keller, Marcel. "MP-SPDZ: A versatile framework for multi-party computation." In Proceedings of the 2020 ACM SIGSAC conference on computer and communications security, pp. 1575-1590. 2020.

[2] Ochiai, Shogo, and Keiichi Iwamura. "New Approach to Dishonest-Majority Secure Multiparty Computation for Malicious Adversaries when n< 2k− 1." In 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), pp. 355-361. IEEE, 2020.

[3] Kamal, Ahmad Akmal Aminuddin Mohd, and Keiichi Iwamura. "(Server-Aided) Two-Party Multiplication of Encrypted Shares Using (k, n) Threshold Secret Sharing With N≥ k Servers." IEEE Access 9 (2021): 113117-113129.

[4] Kamal, Ahmad Akmal Aminuddin Mohd, and Keiichi Iwamura. "Searchable encryption using secret sharing scheme that realizes direct search of encrypted documents and disjunctive search of multiple keywords." Journal of Information Security and Applications 59 (2021): 102824.

[5] Iwamura, Keiichi, and Ahmad Akmal Aminuddin Mohd Kamal. "Secure Computation by Secret Sharing using Input Encrypted with Random Number." In SECRYPT, pp. 540-547. 2021.

[6] Huang, Kai, Ximeng Liu, Shaojing Fu, Deke Guo, and Ming Xu. "A lightweight privacy-preserving CNN feature extraction framework for mobile sensing." IEEE Transactions on Dependable and Secure Computing 18, no. 3 (2019): 1441-1455.

[7] Ragab, Hany, Alyssa Milburn, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida. "Crosstalk: Speculative data leaks across cores are real." In 2021 IEEE Symposium on Security and Privacy (SP), pp. 1852-1867. IEEE, 2021.

[8] Van Schaik, Stephan, Marina Minkin, Andrew Kwong, Daniel Genkin, and Yuval Yarom. "CacheOut: Leaking data on Intel CPUs via cache evictions." In 2021 IEEE Symposium on Security and Privacy (SP), pp. 339-354. IEEE, 2021.

[9] Liu, Yang, Zhuo Ma, Ximeng Liu, Siqi Ma, and Kui Ren. "Privacy-preserving object detection for medical images with faster R-CNN." IEEE Transactions on Information Forensics and Security 17 (2022): 69-84.

[10] K. Iwamura, A. A. A. Mohd Kamal, and M. Inamura, ``TTP-aided secure computation using secret sharing with only one computing server," in Proc. ACM Asia Conf. Comput. Commun. Secur. New York, NY, USA: Association for Computing Machinery, May 2022, pp. 1243_1245.