International Journal on Applications in Engineering and Technology
Volume 8 : Issue 2 : May 2022, pp 93 – 98 www.aetsjournal.com
ISSN (Online) : 2455 - 0523

IMPROVED DATA SECURITY WITH MULTIPLE SECRET SHARING USING XOR VISUAL CRYPTOGRAPHY

BHUVANESH.L, DINESH KUMAR.R, RAMU.Y, NATHIYA.N

[1, 2, 3] Undergraduate student, Department of Computer Science and Engineering, Pavai College of Technology
[4] Assistant Professor, Department of Computer Science and Engineering, Pavai College of Technology

Abstract: *- –* Information/data hiding is a mechanism which ensures that the presence of the secret data remains undetected. Two types of data hiding techniques are most popular, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography process hides message into cover file and forms a stego file. In image steganography there is a need of method which will increase the security, reduce the distortion in the stego file and recovers the data without any loss. In the era of multimedia and internet there is need of reducing time for transmission. 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. The secret text was hidden within secret image. The secret image can be obtained by super imposing the random shares. Conventional n out of n visual cryptography scheme is used to convert a single image into n shares. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. A text is written and hidden inside an image. LSB method is used for this purpose. Now the image is splitted into shares. Each share is 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.

Key words: Cryptography, Visual, Data Security, Secret Key, Steganography

I. INTRODUCTION

Steganography is the practice of hiding secret messages (hidden text) within every day, seemingly innocuous objects (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.

1.1STEGANOGRAPHY WORKNG PROCESS

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.

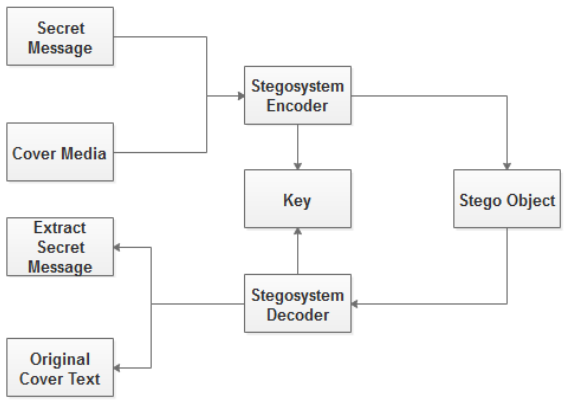


FIG:1PROCESSING STEPS FOR STEGANOGRAPHY

1.2 OBJECTIVE

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 (know 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.

1.3 LITERATURE

This section examines educational expert recommender systems in-depth, with a focus on career-path recommenders. There are many different sorts and categories of recommender systems that are used to help students and teachers learn. This review, however, will concentrate on personalized fuzzy recommender systems for various disciplines and educational levels. We advise the reader to some good reviews from the literature [17]–[19] for further information on different sorts of recommenders. The deployment of tailored recommender systems is influenced by several elements, including the target users' profiles, gender, environmental and cultural background, and personality type. Table 1 summarizes the different forms of personalized recommender systems and their implementation for a better understanding of the different types of personalized recommender systems.

II. SYSTEM ANALYSIS

2.1 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. This method strictly relies on the properties of secret sharing. Summarizing the main techniques, secret sharing serves as the underlying primitive offering security, multiple secret preserves size complexity, and inherently additive homomorphism realizes the data embedding. Here provide the formal description of the technique, and present a clear notion, so-called operating addition homomorphism in multi-secret sharing (OAMSS). Also provide another technique to compress the size of a key used in OAMSS. For generalization, if SNK (Share No Secret Key) schemes satisfy some properties, they can be converted to SOK (Share One Key). Hence, this method can be generalized as a converter. As a concrete instantiation, SNK scheme based on difference expansion, we show the SOK-type RDHEI by slight modification.

2.1.1 DISADVANTAGES

The proposed method needs to switch operations on different marked encrypted images, and hence it takes more time in decryption.Sharing multiple shares will increase extra computational consumption.For the content-owner and the receiver, the expansion rates increase linearly.

2.2 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. The secret text can be hidden within the image 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 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 LSB method.

2.2.1 ADAVANTAGES

The secret image and the recovered image will be of the same size.Multi secret sharing is used to send multiple shares at the same time.Enhance security with XOR algorithm.To retain the quality of the recovered image.

ISSN (Online) : 2455 - 0523

III. SYSTEM SPECIFICATION

3.1 FEASIBILITY STUDY

The feasibility Analysis is an analytical program through project manager determines the project success ratio and through feasibility study project manager able to see either project.

3.1.1 ECONOMICAL FEASIBILITY

Hence this project is economically feasible there is no need to involve any cost for this project.

3.1.2 TECHNICAL FEASIBILITY

Software Technologies used are JSP and MYSQL. In the educational institutions, it is possible to update the system in future. No special hardware is required for the purpose of using this system. Hence it is declared that this project is technically feasible.

3.1.3 OPERATIONAL FEASIBILITY

In training phase, easy to train the animal datasets and provide alert system in real time environments. Hence it is easy to operate with training. Therefore it is operationally feasible for implementation.

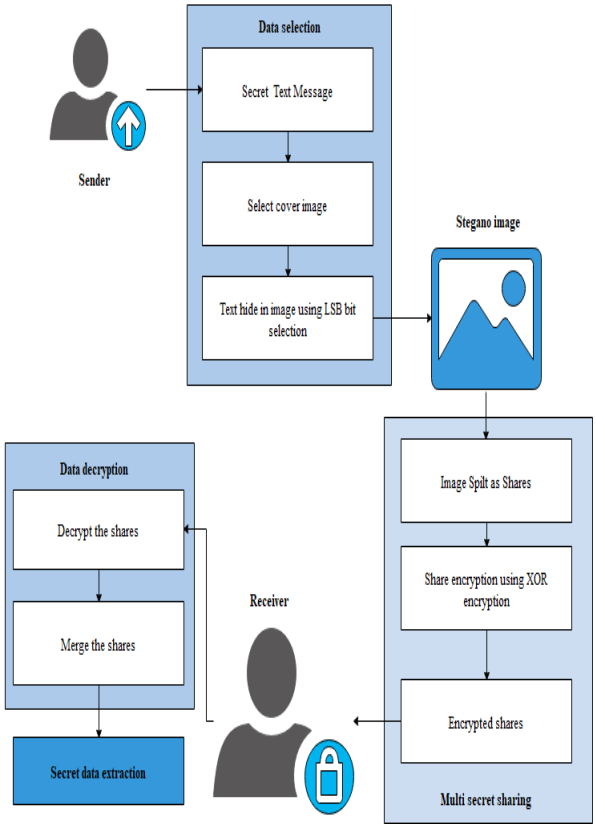
3.3.1.4 ENVIRONMENTAL FEASIBILITY

This project environment is correct as user has developed this system and no expenditure is involved under any head and this process is part of admin document management, this project environment is accessible.

IV. SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

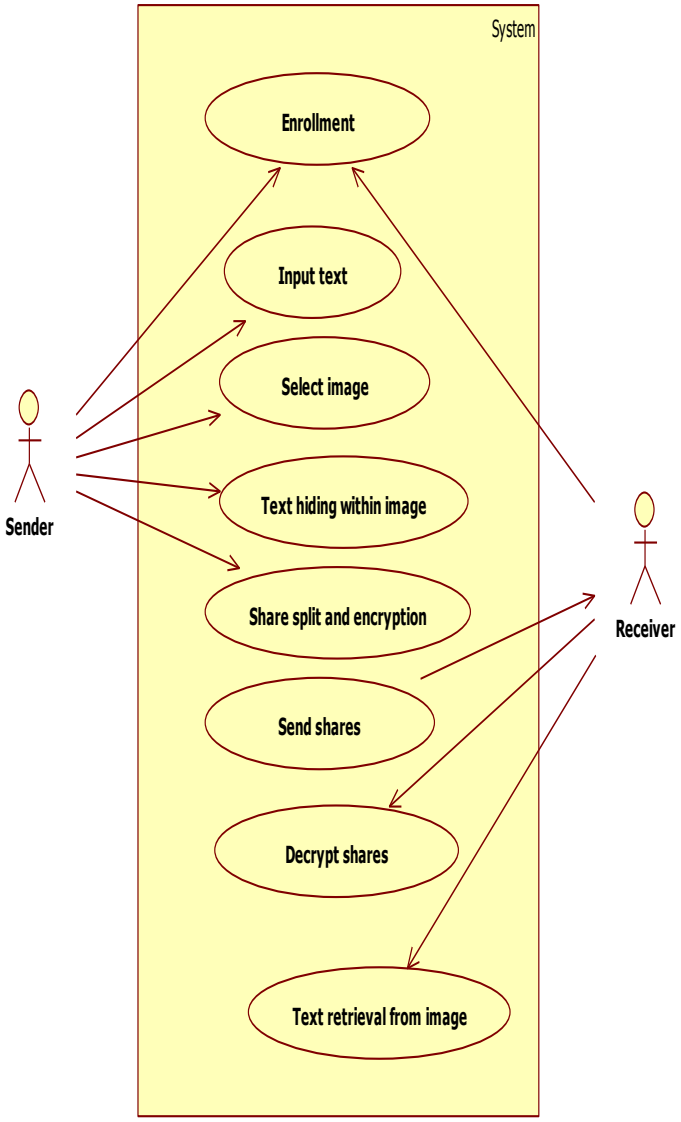
System architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. In this architecture, sender can send the secret text message and select the cover image. Then hide the image using LSB bit selection and encrypt the image using XOR operation. Then split image as shares. In receiver side, merge the splits and decrypt the image. Finally extract the secret text from image.



4.2 USECASE DIAGRAM

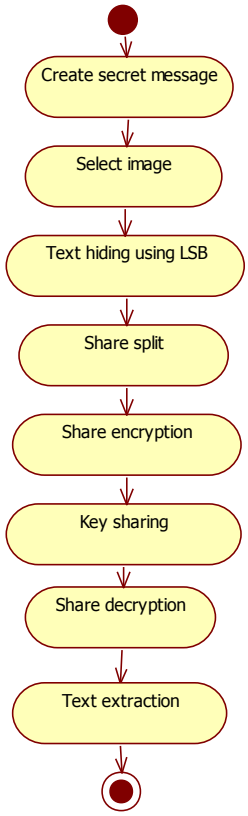
In software and systems engineering, a use case is a list of steps, typically defining interactions between a role (known in UML as an "actor") and a system, to achieve a goal. The actor can be a human or an external system. In systems engineering, use cases are used at a higher level than within software engineering, often representing missions or stakeholder goals. The detailed requirements may then be captured in Sys ML or as contractual statements

ISSN (Online) : 2455 - 0523



4.3 ACTIVITY DIAGRAM

Activity diagram is another important diagram in UML to describe dynamic aspects of the system. Activity diagram is basically a flow chart to represent the flow form one activity to another activity. The activity can be described as an operation of the system. So the control flow is drawn from one operation to another. This flow can be sequential, branched or concurrent. Activity diagrams deals with all type of flow control by using different elements like fork, join etc. The basic purposes of activity diagrams are similar to other four diagrams. It captures the dynamic behaviour of the system.



V. MODULE DESCSRIPTION

5.1.1ENROLMENT AND FILE SHARING

Enrolment is the process of registering in application to get access permission. Then sender could create text message for sharing to the receiver. The secret text message hiding is a process of embedding the secret text imperceptibly into the cover media by minimally modifying the elements of the cover media. In this module sender will generate the content for transmit to the receiver.

5.1.2 IMAGE UPLOAD AND HIDING

This process is to select cover media for information hiding. Here images are used as a cover media for the secret message. Cover image is also select by the sender when create the secret message. Original message is hidden into the cover media (image) to improve the security of data sharing. The steganographed image that has to sent should be uploaded. The image should be any one of the image supporting formats. A text is written and hidden inside a secret image. This is done by using modified LSB method. The cover image is called as a steganographed image.

5.1.3 SHARE SPLIT AND ENCRYPTION

The uploaded image will be divided into "n" number of shares according to the user requirements. "n" is the product of rows and columns. Here, in this project, the number of shares is 16 (4*4). Maximum number of shares is fixed to 8 * 8. Splited image shares will be encrypted separately using XOR method. A key is used to encrypt the shares. Exclusive-or encryption requires that both encryptor and decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is nearly unbreakable. That key will be mailed to the receiver. If JPEG image is used, the encrypted share will be in black and white color. It will look like a QR code.

5.1.4 MULTI SHARE SENDING

All the individual encrypted shares will be stored in a folder. By using this module, all the encrypted shares will be sent to the receiver in a single transmission. This single transmission enables receiver to receive all the shares at a time. This will helps to avoid the information or share missing and also it saves transmission and receiving time for both sender and receiver.

5.1.5 SHARE DECRYPTION AND DATA EXTRACTION

All the encrypted shares will be received by the receiver in a single transmission. Each received share will be decrypted individually using inverse XOR method. The key that is received through mail is used in this decryption process. Private key is used for both encryption and decryption process. The output of this module will be an individual share in the decrypted form. All the decrypted individual shares are the input for this module. These individual shares will be joined together to form the original (secret) image. The recovered image can be viewed as a complete single image. The dimensions of both the original image and the recovered image will be the same. The hidden text file will be recovered from the secret image. Receiver gets the secret message with cover text. LSB method is used to retrieve the hidden text Specific key is generated and shared to the receiver during the process of message sending. Receiver can decrypt the text using shared secret key. Then the original message is shown to the receiver.

5.2 SYSTEM TESTING

5.2.1 Unit Testing

Unit testing comprises the set of tests performed by an individual programmer prior to integration of the unit into a larger system. The module interface is tested to ensure that information properly flows into and out of the program unit. The local data structure is examined to ensure that data stored temporarily maintains its integrity during all steps in an algorithm's execution. Boundary conditions are tested to ensure that the module operates properly at boundaries established to limit or restrict processing. All independent paths through the control structure are tested. All error-handling paths are tested.

VI. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was creates by sender then select the cover image to hide the secret message using LSB approach that should be sent the message secretly to the receiver. Then the secret image is splitted 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.

VII. FUTURE ENHANCEMENT

In future work authentication has to improve using different algorithms and recovered image size should be considering as same for shared image. Also the noise level should be decreased and encryption and decryption time of multiple shares can be calculating for improve the performance.

REFERENCES

[1]. Chen, Yu-Chi, "A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms." IEEE Transactions on Information Forensics and Security 14, no. 12 (2019): 3332-3343.

[2]. Liao, Xin, and Changwen Shu. "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels." Journal of Visual Communication and Image Representation 28 (2015): 21-27.

[3]. Wu, Hao-Tian, "High-capacity reversible data hiding in encrypted images by bit plane partition and MSB prediction." IEEE Access 7 (2019): 62361-62371.

[4]. Yi, Shuang, and Yicong Zhou. "Parametric reversible data hiding in encrypted images using adaptive bit-level data embedding and checkerboard based prediction." Signal Processing 150 (2018): 171-182.

[5]. Bartwal, Monika, and Rajendra Bharti. "Lossless and Reversible Data Hiding in Encrypted Images With Public Key Cryptography." Annals of Computer Science and Information Systems 10 (2017): 127-134.

[6]. Dragoi, Ioan Catalin, Henri-George Coanda, and Dinu Coltuc. "Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction." In 2017 25th European Signal Processing Conference (EUSIPCO), pp. 2186-2190. IEEE, 2017.

[7]. Qian, Zhenxing, "Separable reversible data hiding in encrypted JPEG bitstreams." IEEE Transactions on Dependable and Secure Computing 15, no. 6 (2016): 1055-1067.

[8]. Liu, Jianyi, Kaifeng Zhao, and Ru Zhang. "A fully reversible data hiding scheme in encrypted images based on homomorphic encryption and pixel prediction." Circuits, Systems, and Signal Processing (2019): 1-21.

[9]. Zhou, Jiantao, Weiwei Sun, Li Dong, Xianming Liu, Oscar C. Au, and Yuan Yan Tang. "Secure reversible image data hiding over encrypted domain via key modulation." IEEE transactions on circuits and systems for video technology 26, no. 3 (2015): 441-452.

[10]. Wu, Han-Zhou. "Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification." IEEE transactions on circuits and systems for video technology 27, no. 8 (2016): 1620-1631.

BIOGRAPHIES

BHUVANESH.L is an undergraduate student ,department of computer science and engineering in paavai college of engineering

DINESH KUMAR.R is an undergraduate student ,department of computer science and engineering in paavai college of engineering

RAMU.Y is an undergraduate student ,department of computer science and engineering in paavai college of engineering.

Mrs.N.NATHIYA M.E(P.hd) is an assistant professor in paavai college of engineering