EasyChair Preprint

№ 5256

Multi Secret Sharing with Encrypted Data Hiding for Secure Communication

S Jegadeesan, K S Naghulkirthic, K Akash and K Akash

March 31, 2021

MULTI SECRET SHARING WITH ENCRYPTED DATA HIDING FOR SECURE COMMUNICATION

Dr.s.Jegadeesan [1], K.S.Naghul kirthik [2] , K.akash [3], , K.akash [4]
Assistant Professor[1], UG Scholar[2,3,4]
Department of Electronics and Communication Engineering,
M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India.

Abstract*—Visual Cryptography (VC) is a technique for breaking an image into two random shares, each of which reveals no details about the hidden image when viewed separately. By superimposing the two shares, the hidden picture can be obtained.To encrypt a single image into n shares, a standard visual cryptography scheme is used. Only shares can be used to decode the image. For this procedure, many visual cryptographic methods only use binary images. This is inconvenient for many applications. First, access structures for a single secret are converted into access structures for several secrets.A necessary condition for MSS (Multiple Secret Sharing) schemes realising an access structure for multiple secrets of the most general form is added, and two MSS scheme constructions with encryption that satisfy this condition are given implementation. .Each of the two constructions has a distinct benefit over the other: one is more general and can generate MSS schemes with stricter contrast and pixel expansion than the other, while the other has a simple interface.

I. INTRODUCTION

Steganography is a method of concealing information. art of concealing coded notifications (hidden text) inside everyday, apparently harmless an item (cover text)in order to create a stego text. The receiver of a stego text will retrieve the secret text from the stego text using his knowledge of the steganography system used.The aim the goal of steganography is to encourage parties involved in communicate covertly in such a way that an attacker cannot deduce whether or not their communication contains hidden meaning. This distinguishes steganography from cryptography, which, while allowing for private communication, can raise suspicion simply by virtue of its use.

Steganography substitutes bits of new and invisible information for unneeded or unused bits in standard computer files (graphics, sound, and text). Any other standard computer file or encrypted data may be used to hide information. Steganography varies from cryptography in that it conceals the message's presence, while cryptography conceals the message's material.Steganography is often combined with encryption.Even if the encrypted file is deciphered, the secret data can be hidden using steganography, so the hidden information is not visible.

II. RELATED WORK

a.Symmetric-key Cryptography

A Both the sender and the receiver use the same token. The sender uses this key to encrypt plaintext and return the code text to the receiver. The recipient, on the other hand, deciphers the message and recovers the plain content using a similar token.. A single key is used for both encryption and decoding in symmetric cryptography. A sender and a beneficiary should already have a shared key that they all know. Key dispersion is a fascinating topic that inspired the creation of lopsided cryptography. Two different keys are used for encryption and decoding in topsy-turvy crypto. In a deviated cryptosystem, each client has a public and a private key The private key is still kept secret, but the public key is not. can be freely circulated. With the comparing private key, data encoded with a public key can be decoded. Having an impression on John, in this case, necessitates encoding the message with John's public key. Since only John has his private key, no one else can decipher the message. With the contrasting public key, any information encoded with a private key must be decoded. Jane could also use her private key to carefully sign a letter, and someone with Jane's public key could decrypt the message and verify that it was, in fact, Jane who sent it. Symmetric is, for the most part, incredibly fast and suitable for scrambling large amounts of data (e.g., a whole page of text). Hilter kilter is becoming increasingly sluggish because it only scrambles bits of data that are smaller than the key size (normally 2048 pieces or more modest). Along these lines, lopsided cryptography is most commonly used to encrypt symmetric

encryption keys, which are then used to scramble much larger squares of data. Deviated crypto is widely used to scramble the hashes of advanced labels. The age, exchange, stockpiling, use, repudiation, and replacement of cryptographic keys are all handled by a cryptosystem.

b. Public-Key Cryptography

This has become the most radical idea of the past 300-400 years. In public-key cryptography, two related keys (public and private keys) are used. The public key can be publicly distributed, but the merged private key is unknown. The public key is used to encrypt data, while the private key is used to decrypt data.Public-key cryptography, also known as deviated cryptography, is a type of encryption that uses public keys. . Unlike symmetric key calculations, which rely on a single key to both scramble and unscramble, each key performs a specific function. The public key is used to encrypt, and the private key is used to decrypt. It is computationally impossible to calculate the private key based on the public key. As a result, public keys can be freely exchanged, allowing clients an easy and ad hoc authentication procedure and efficient method for scrambling content and checking advanced marks, and private keys can be kept secret, meaning that only the owners of the private keys can unscramble content and make computerized marks.

III. EXISTING SYSTEM

c.description

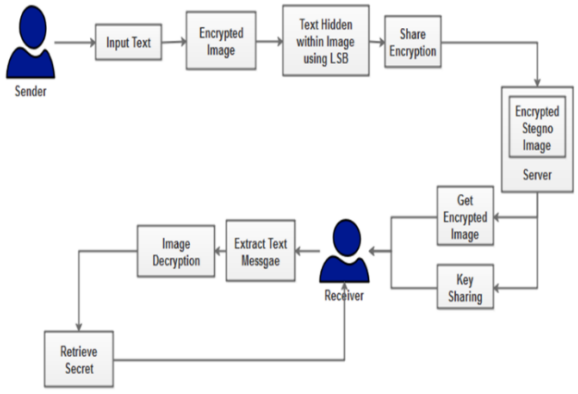
RHD-EI enables a server to embed a message into an encrypted image submitted by the content owner, ensuring that the first content are often retrieved without loss after decryption on the receiver hand.

This approach is entirely based on hidden sharing properties. To summarise the key techniques, secret sharing is the underlying primitive that provides protection, multiple secret retains size complexity, and data embedding is realised using inherently additive homomorphism. Provide a formal definition of the technique as well as a simple concept, referred to as operating addition homomorphism.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). As a result, this approach can be used as a converter. We display the SOK-type RDHEI by minor modification as a concrete instantiation of the SNK scheme based on difference expansion. The following may be a summary of the scheme. P can use polynomial interpolation to offer H the encrypted image after pre-processing the cover-image and generating a replacement cover-image, mentioned because the processed image. H can obtain a replacement polynomial containing a hidden message inside the published LSB plane, and then use extension homomorphism to obtain the encrypted image with embedded message Finally, by decryption, R is able to obtain the stego-image, as well as the cover-image and secret. message.

d.Disadvantages

- It suffers from extreme data expansion and high computational complexity..
- It does not allow multiple hidden sharing in a single transmission..
- Increase the embedding ability as high as possible for image distortion..

EXISTING SYSTEM BLOCK DIAGRAM



IV. PROPOSED SYSTEM

e.DESCRIPTION

The primary goal of this venture is to build up secure correspondence between the sender and the recipient using messages and different methods of correspondence. In this paper, a XOR-based multi secret sharing plan is proposed for safely sending pictures from the source to the objective. This technique dispenses with the key security difficulties of VC like outside utilization of code book, arbitrary offer examples, pixel extension in shared and recuperated pictures, lossy recuperation of mystery pictures, and share count limitation. The proposed method is n out of n secret sharing schemes. This proposed work allows for the simultaneous transmission of multiple secret images. Text files containing the secret text were present. The sender will create that file in order to send it to the receiver. Only when all n shares are received and decrypted by the receiver can the secret image be revealed. The text has been typed and is hidden within an image. This is

accomplished through the use of the Modified LSB method. The image is then encrypted and sent to the receiver using the XOR-based VC method. The key needed to encode the offers will be sent to the beneficiary. The offers will be decoded by the collector utilizing the very key that was utilized for encryption. The hidden text will then be extracted from the recovered image using the Modified LSB method.

f. Enrolment and File Sharing

The text has been typed and is concealed by an image. This is accomplished by employing the Modified LSB method. Using the XOR-based VC method, the image is then encrypted and sent to the receiver. The recipient will get the key needed to encode the offers. The beneficiary will decode the offers utilizing the very key that was utilized for encryption. The secret content will at that point be uncovered.

1. Image Upload and Hiding

This procedure involves the selection of cover media for the concealment of information. Images are used as a cover media for the secret message in this case. When creating a secret message, the sender can also choose a cover image. To improve data sharing security, the original message is hidden within the cover media (image). The steganographed image that must be transmitted should be uploaded. Any of the image suggestions should be used as the image.formats that are compatible A text is written and concealed within a hidden image. This is accomplished through the use of the LSB method. A steganographed image is the name given to the cover image.

2.MPVD with LSB Algorithm

A cover image is separated into nine consecutive non-overlapping pixels blocks.during the embedding process of a secret message.

- A distinction esteem is processed by taking away the estimations of the nine pixels in each square.
- All conceivable distinction esteems are separated into a few reaches. The determined contrast esteem is then supplanted with another worth to install the estimation of a sub-stream of the mysterious message.
- The quantity of pieces that can be inserted in a pixel pair is controlled by the width of the distinction worth's reach.

.LSB insertion refers to the method of embedding the secret information within the cover file. The binary representations of the secret data were taken in the proposed technique, and the LSB of each byte was overwritten within the image small.

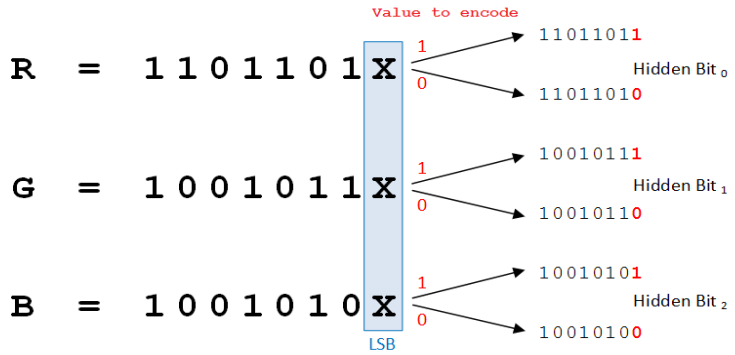


Fig4.2. LSB Steganography

3.LSB Encoding

First, the one-of-a-kind picture and the packed encoded secret message are caught. The scrambled mystery realities should then be changed over into paired configuration. Twofold change is refined by changing over the individual's American Standard Code of Information Interchange (ASCII) values to binary. Layout and bit-movement output Similarly, in the cover photo, pixels are represented by bytes in an unmarried cluster, and a byte stream is created. Message pieces are taken successively and afterward positioned in the LSB bit of a picture byte. A similar methodology is rehashed until the entirety of the message pieces are situated in photo bytes. The picture that is made is known as a 'Stego-Image.' It is prepared for transmission.

The following is an algorithm for concealing enigmatic facts in the cover image:

Step 1: Read the cover media photograph as well as the confidential information that will be embedded in the image.

Step 2: Condense the hidden information.

Step 3: Utilizing the mysterious key shared by the recipient and sender, convert the packed privileged insights into figure text based substance.

Step 4: Make a binary representation of the compressed encrypted textual content message.

Step 5: Compute the LSB an incentive for each RGB pixel in the cover picture.

Step 6: In the RGB pixels of the cover picture, install the pieces of the restricted information into the LSB bits.

Step 7: Rehash Steps 1–7 until the cover report's restricted data is totally covered up.

4.LSB Decoding

During the encoding process, a 'Stego-Image' is created first, and a single array of bytes is

generated.. The bytes representing Thestego-image pixels and the total number of bits of encrypted secret information are counted. The counter is originally set to 1, indicating the pixel byte index range where the hidden message bit is located. can be found in LSB. The operation will be repeatedbefore the very last bit of the hidden message is reached After that, the message's bit circulation will be produced. Bytes are formed by grouping bits together, and each byte represents a single ASCII character.The encoded embedded message is represented by characters in a textual content record. Following that, as well as decryption and decompression are two steps in the decryption and decompression process. must be completed.

The following is an algorithm for exposing hidden data in a Stego image:

Step 1: Take a look at the stego pic.

Step 2: Calculate the LSBs for each RGB pixel in the stego image.

Step 3Find the LSBs of each RGB pixel in the stego picture and recover them.

Step 4: Rehash the interaction until the message has been totally separated from the stego picture.

Step 5: Decompress the hidden facts that have been collected.

Step 6: Decrypt secret records using the shared key to obtain original records.

Step 7: Reassemble the hidden figures.

g. Share Split and Encryption

According to the user's preferences, the uploaded image will be split into "n" number of shares. The product of rows and columns is “n.” The number of shares in this project is 16 (4*4). The maximum number of shares is 8 * 8. The XOR form will be used to encrypt the split image shares separately. The shares are encrypted using a key. Exclusive-or encryption necessitates the presence of both the encryptor and the decryptor approach the encryption key, however the encryption calculation is practically strong, despite its simplicity. The recipient will receive the key via mail. The encrypted share would be black and white if a JPEG image is used. It will have the appearance of a QR code.

1.XOR Encryption Algorithm

Exclusive-OR encryption is nearly unbreakable using brute force methods, despite not being a public-key system like RSA. It is vulnerable to patterns, but this flaw can be mitigated by compressing the file first (so as to remove patterns). encryption or exclusivity necessitates that both The encryption key is accessible to both the encryptor and the decryptor, but despite its simplicity, the encryption algorithm is nearly unbreakable. The exclusive-OR boolean algebra function is the foundation of exclusive-OR encryption. (XOR). The XOR administrator is a two-dimensional administrator (implying that it takes two contentions - like the expansion sign, for instance). Or on the other hand, Exclusive-OR,as the name suggests, is a type of conditional logicIf one, and only one, of the two operators is valid, it will return Exclusive-OR encryption is correct.It is based on the assumption that reversing the procedure without understanding one of the two arguments' initial value is unlikely. When two variables are XOR you get with unknown values, for example, you won't be able to say what their values are from the output. Take, for example, the operation A XOR A is TRUE and B is FALSE. Furthermore, even though it returns FALSE, you have no way of knowing whether all values were TRUE or FALSE.

In contrast to logical-AND and logical-OR, in the event that you know either An or B, it's totally reversible. In the event that you run A XOR TRUE and get an estimation of TRUE, you realize An is FALSE, and on the off chance that you get an estimation of FALSE, you realize An is valid. Restrictive OR haphazardly produced keys and endeavoring every one until the yield of the unscrambling programme resembles readable text. The more difficult it is to make an encryption key, the longer it takes. it is to crack. Exclusive-OR encryption works by taking the key and encrypting a file by applying the key to the file's consecutive segments and storing the result.will be it take to decrypt the data using brute force?

Exclusive-OR (XOR) encryption is a type of encryption that is difficult to crack using so-called "brute force" methods (brute force = randomly picking encryption keys in the hopes of finding the right one), but it is vulnerable to pattern recognition. By compressing the file first, patterns can be easily avoided. (compression already makes it unreadable, it removes patterns for you) before it is encrypted.

will it take to decrypt the data using brute force?

Exclusive-OR (XOR) encryption is a type of encryption that is difficult to crack using so-called "brute force" methods (brute force = randomly picking encryption keys in the hopes of finding the right one), but it is vulnerable to pattern recognition. By compressing the file first, patterns can be easily avoided..

2.Share Encryption

Input: An Image
Output: Encrypted Shares
Select an image
Split into n shares (rows & columns)
Begin
Each share = a * b pixels (a – height, b – width)
For i=0 to a
For j=0 to b
Do
Calculate RGB value for each pixel
Convert to byte
Enter key to encrypt
Convert key to byte
Enc byte = (Byte value) XOR (key)

Replace RGB value by Enc byte value for each pixel
Repeat the same procedure for all shares
End

3.Decryption

Input: Enc Shares
Output: An image
Begin
Each Share = a*b pixels (a – height, b – width)
For i=0 to a
For j=0 to b
Do
Calculate RGB value for each pixel
Convert to byte
Enter key to decrypt
Convert to byte
Dec byte = (Byte value) XOR (key)
Convert Dec byte to RGB value for each pixel
Join all shares
End

h. Multi Share Sending

A folder will be created to hold all of the encrypted shares. Both encrypted shares will be sent to the receiver in a single transmission if this module is used. The receiver will receive all of the shares at once thanks to this single transmission. This will help to avoid missed information or sharing, as well as saving both sender and receiver time during transmission and reception.

i. Share Decryption and Data Extraction

The receiver will receive all of the encrypted shares in a single transmission. Each received share will be independently decrypted using inverse XOR method. In this decryption process, the key received via mail is used.. Private key is used for both encryption and process of decryption This module will generate a decrypted individual share as its output. Individual shares that have been decrypted are the input for this module. The original (secret) picture will be created by combining these individual shares. The restored image can be viewed as a single, full image. Both the original and restored images would have the same proportions..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 During the message sending process, a unique key is created and shared with the recipient. The text can be decrypted by the receiver using the shared secret key. The receiver is then shown the original message.

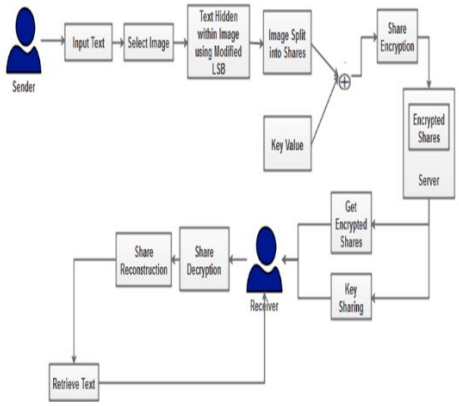
1.Advantages

The secret picture and the recuperated picture will be of a similar size.

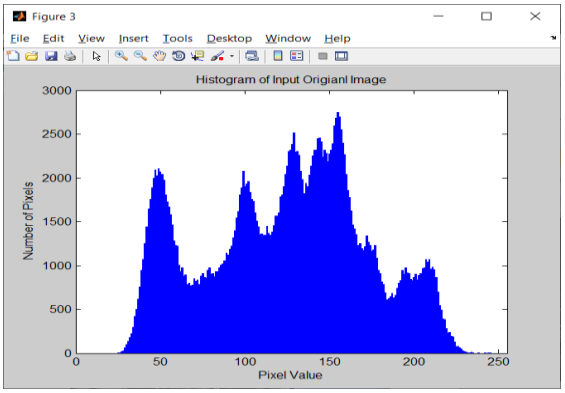
- Multi secret sharing is utilized to send various offers simultaneously.

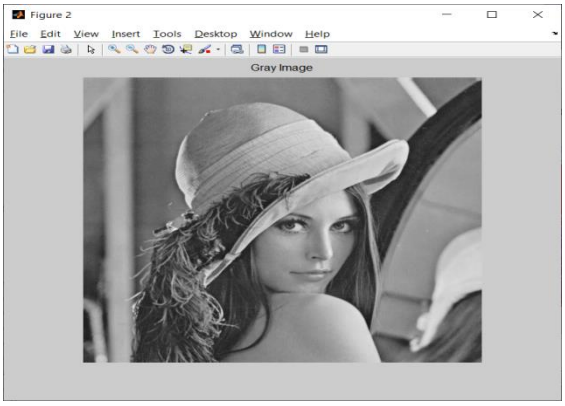
- Enhance security with XOR calculation.

PROPOSED SYSTEM BLOCK DIAGRAM

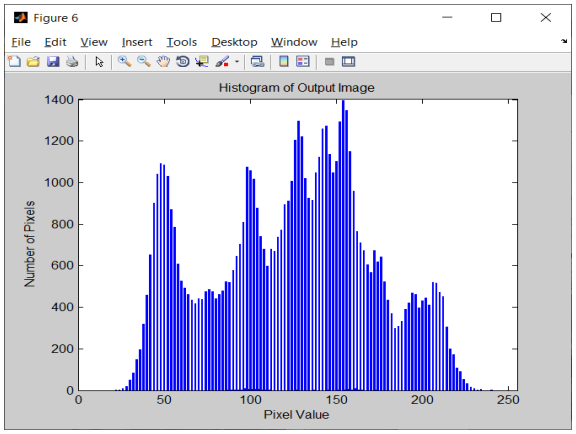


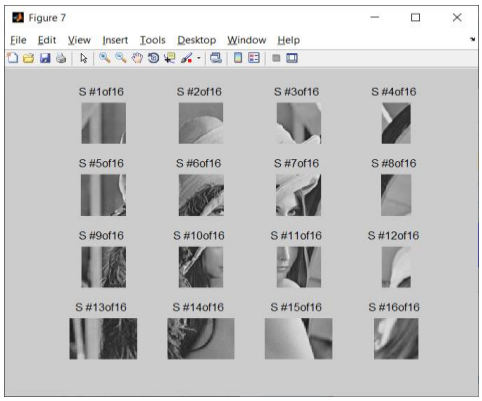
4.f.Encrypted image





j.Decrypted image





S

OUTPUT IMAGE

```
Enter the Key for text encryption  485

Encryption Time
Elapsed time is 0.008688 seconds.

Input Text
This is MATLAB.!

New Encrypted Text
kyzj zj drkcrs.!

Parameter Metrics of Embedded Image Analysis
Mean    : 0.5746
SD      : 0.3796
SSIM    : 0.9983
MS-SSIM: 1.0000
```

CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. In this work, a text message was hidden within QR Code then the QR will be hidden within image. The sender has to create text and generate QR for input text then select the image to hide the QR image using MPVD with LSB approach that ought to be sent the message covertly to the recipient. At that point the mysterious picture is splitted into "n" number of offers. Each offer is encoded utilizing XOR activity. At that point, every one of the scrambled offers are communicated in a solitary transmission to the beneficiary. The collector should utilize the decoding key to unscramble the offers. In the wake of decoding, the individual offers will be consolidated to shape the recuperated (unique) picture. The recuperated picture will be of a similar size as the first picture..

REFERENCES

[1] 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.

[2] Zhang, Xinpeng, Jing Long, Zichi Wang, and Hang Cheng. "Lossless and reversible data hiding in encrypted images with public-key cryptography." IEEE Transactions on Circuits and Systems for Video Technology 26, no. 9 (2015): 1622-1631.

[3] Dragoi, IoanCatalin, Henri-George Coanda, and DinuColtuc. "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.

[4] Yi, Shuang, and Yicong Zhou. "Binary-block embedding for reversible data hiding in encrypted images." Signal Processing 133 (2017): 40-51.

[5] Cao, Xiaochun, Ling Du, Xingxing Wei, Dan Meng, and XiaojieGuo. "High capacity reversible data hiding in encrypted images by patch-level sparse representation." IEEE transactions on cybernetics 46, no. 5 (2015): 1132-1143.

[6] Chuman, Tatsuya, Kenta Kurihara, and Hitoshi Kiya. "On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks." IEICE TRANSACTIONS on Information and Systems 101, no. 1 (2018): 37-44.

[7] Kobayashi, Hiroyuki, and Hitoshi Kiya. "Bitstream-Based JPEG Image Encryption with File-Size Preserving." In 2018 IEEE 7th Global Conference

on Consumer Electronics (GCCE), pp. 384-387. IEEE, 2018.

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

[9] Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. "New framework for reversible data hiding in encrypted domain." IEEE transactions on information forensics and security 11, no. 12 (2016): 2777-2789.

[10] Xiang, Shijun, and XinrongLuo. "Reversible data hiding in homomorphic encrypted domain by mirroring ciphertext group." IEEE transactions on circuits and systems for video technology 28, no. 11 (2017): 3099-3110.