International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 5 ǁ May 2023 ǁ PP. 94-99

Enhance the Security of Data Using Cryptographyin Data Hiding Using Pixel Rotation

S.Uma[1], R.Priyadharshini[2], R.Shalini[3]
[1]*Assistant Professor, Computer Science And Engineering, Paavai Engineering College, Tamil Nadu, India*
[2,3]*Student, Computer Science And Engineering , Paavai Engineering College, Tamil Nadu, India*

ABSTRACT
It is necessary to provide an easy and safe way to protect messages from being hacked due to the availability of several social media platforms and their use for text messaging. This is especially true in the presence of intruders and data thieves, and considering that the majority of messages are private and confidential, it is necessary to provide an easy and safe way to protect messages from being hacked. A straightforward approach to message cryptography will be proposed in this research paper. A message is broken up into predetermined block sizes using this method. From two to sixty blocks are available. An array of a size proportional to the number of blocks produced is created through the use of a secret color image. After that, the array will be utilized as a private key. In order to perform the block rotation left operation, each component of the private key will be used to calculate the number of rotation digits for the associated block. The following parameters will be used to evaluate the proposed method: Throughput, the correlation coefficient (CC), the peak signal- to-noise ratio (PSNR), and the mean square error (MSE). Data Encryption Standard (DES), Triple- DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF) are among the standard message cryptography methods that will be contrasted with the proposed method. Based on the secret image, block size, and calculated Rotation Left Digits (RLD) for each block, the experimental results demonstrate that the proposed method is sufficiently secure.

Keywords: *Cryptography , XOR based method , Multisharing ,Work authentication.*

Date of Submission: 19-04-2023 Date of acceptance: 03-05-2023

I. INTRODUCTION

Cryptography is a craft of convert correspondence, which offers emit and get method of correspondence. Audio-video synchronization, copyright management, television broadcasting, military use, and digital watermarking are just a few of its many potential applications. People are able to distribute large multimedia files and create identical data copies thanks to broadband internet connections that virtually eliminate data transmission errors. Even though everyone has something they want to keep a secret, sending confidential files and messages over the internet is risky. Cryptography aims to conceal the secret data within the cover medium without affecting its overall quality.

II. RELATED WORKS

Cryptography covers most frequently make use of digital images. The algorithm used fordifferent file formats varies depending on the application and the variety of file formats available. An image is a collection of bytes, or pixels for images, with various light intensities in various areas. While managing computerized pictures for use with Cryptography, 8-bit and 24-bit perpixel picture documents are regular. Both have benefits and drawbacks. Because of their small size, 8-bit images are ideal for use. There are only 256 colors that can be used, which could cause problems during encoding. When working with 8-bit images like.GIF, a gray scale color palette istypically used because the image's gradual color change would be harder to detect once the secretmessage was encoded into it. When used in cryptography, 24-bit images offer significantly moreadaptability. There are more than 16 million colors that can be used, which is a lot more than thehuman visual system (HVS) can see. This makes it very hard to find once a secret message has been encoded.

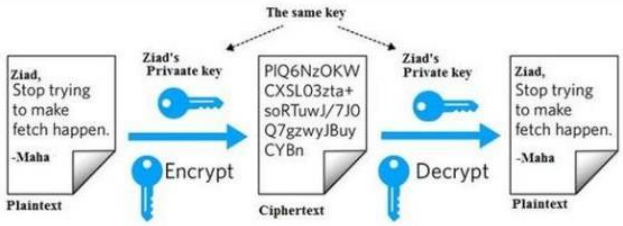

Fig. 1 Data cryptography process.

Huge measure of information can be encoded in to 24-digit pictures as it is contrasted with 8-bit pictures. When compared to 8-bit images, the disadvantage of 24-bit digital images is their large size, which makes them suspicious on the internet. Different algorithms are used depending on the type of message and image.

1.1. Least significant bit insertion

Least Significant Bit (LSB) insertion, which involves altering the LSB layer of the image. The message is stored in the LSB of the pixels using this method, which could be thought of as random noise. As a result, changing them has no obvious effect on the image.

1.2. Masking and filtering

Masking and filtering are more effective with images that are grayscale and 24 bits. They sometimes function as digital watermarks and conceal information in a manner analogous to that ofpaper watermarks.
The images are altered when they are masking. Make the changes in multiple small amounts to ensure that they cannot be detected. Masking is more durable than LSB, and it can handle cropping, compression, and some image processing. The hidden message is incorporated into the cover image more than just hidden in the "noise" level thanks to masking techniques that embed information in important areas.

1.3. Redundant Pattern Encoding

Technique and Redundant Pattern Encoding There are some similarities between the two. The message is distributed throughout the image using this method using an algorithm. The image cannot be cropped or rotated using this method. Even when the stegano-image is manipulated, the likelihood of recovery is increased by multiple redundant smaller images.

1.4. Encrypt and Scatter

White Noise Storm is an example of an encryption and scatter technique that employs spreadspectrum and frequency hopping to conceal the message. Encrypt and Scatter A random number is generated using the previous window size and the data channel. Within this random number, messages are distributed across all eight channels.

Each channel alternates, rotates, and interlaces with each other. Each channel contains numerous unaffected bits because each channel represents a single bit. Drawing the actual message from the stegano image using this method is a very challenging process. Because it requires both an algorithm and a key to decode the bit message from the stegano-image, this method is more secure than LSB. Despite the stegano image, this method requires both an algorithm and a key, so some users prefer it for its security. Similar to LSB, this method permits image processing and compression degradation.

1.5. Algorithms and transformations

Algorithms and transformations The LSB image modification technique works with any compression, such as JPEG or GIF, on the resulting image. The discrete cosine transform is used to compress JPEG images. Because the cosine values cannot be precisely calculated, and repeated calculations with limited precision numbers introduce rounding errors into the final result, DCT is a lossy compression transform. The way DCT is calculated affects the differences between restoredand original data values.

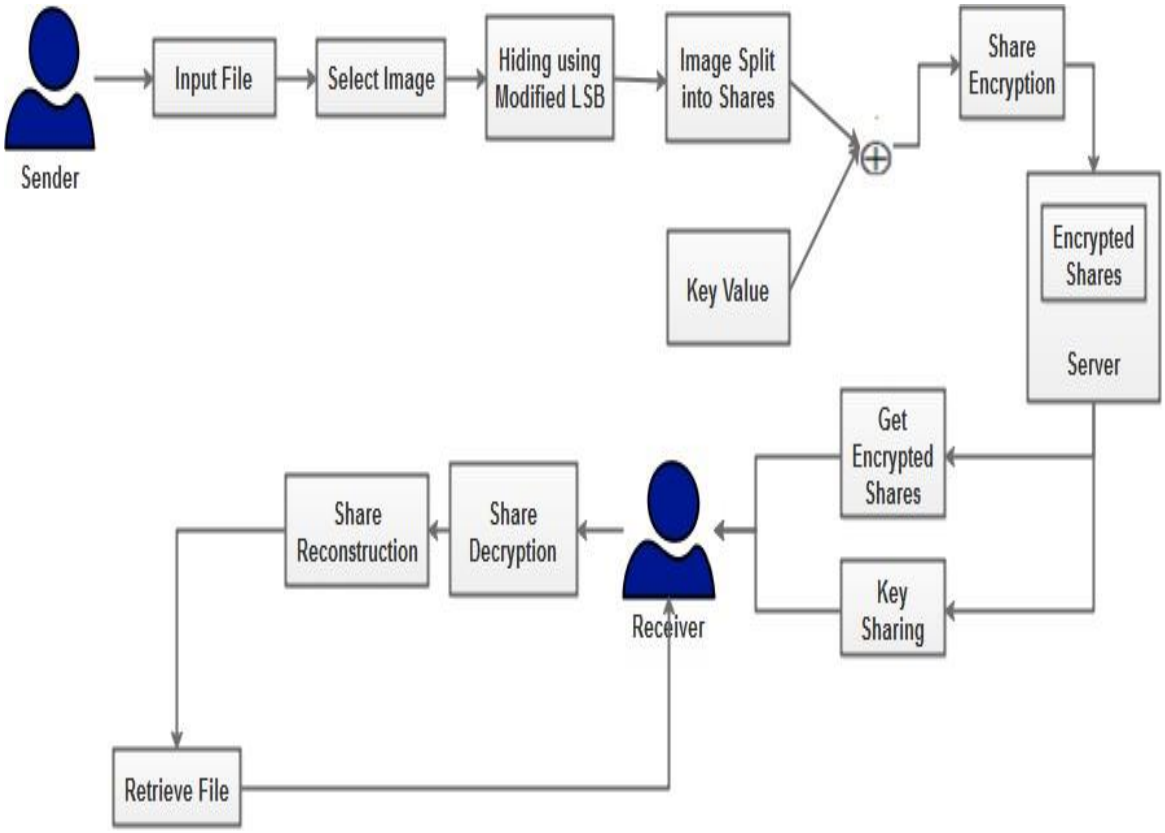

Fig. 2 Proposed System Model

III. PROPOSED WORKS

The primary objective of this project is to use emails and other forms of communication to establish secure communication between senders and recipients. To secure send images from the source to the destination, this work proposes XOR-based multi-secret sharing. External use of the code book, random share patterns, the expansion of pixels in shared and recovered images, lossy recovery of secret images, and a cap on the number of shares are all eliminated by this approach. The proposed approach is a scheme for sharing n out of n secrets. This proposed work allows for the simultaneous transmission of multiple secret images. The sender concealed the text message within the selected cover image file. When all n shares are decrypted and received by the receiver, the secretimage can be seen. In an image, the text is typed and hidden. The Modified LSB method is used for this.

The image is then encrypted and sent to the receiver using the XOR-based VC method. The receiver will receive the key used to encrypt the shares via mail. The shares will be decrypted by the receiver with the same key used for encryption. The Modified LSB method will then be used to extract the hidden text from the recovered image.

1.6. Modified LSB Algorithm

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

- Distinction esteem is determined from these upsides of the nine pixels in each block.
- A variety of ranges are used to group all of the possible difference values.
- A new value was then used in place of the calculated difference value to embed the value of asecret message sub stream.
- The width of the range that the difference value occupies determines the maximum number ofbits that can be embedded in a pixel pair.

LSB insertion is the process of embedding secret information within the cover file. The secret data's binary representations are taken in the proposed method, and the LSB of each byte is overwritten in the image. On the off chance that 24-cycle variety pictures are utilized to performLSB, how much adjustment will be little.

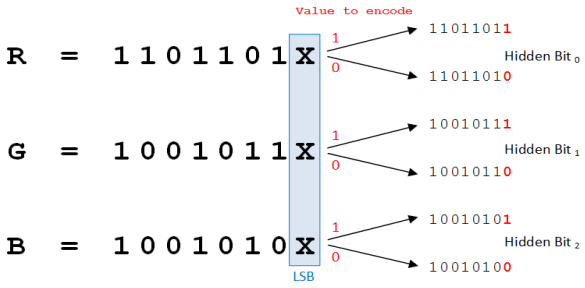

Fig 3 LSB Cryptography

1.7. LSB Encoding

The unique image and encrypted secret message are taken first. The encrypted secret information must then be converted into binary format. By converting the individual's American Standard Code of Information Interchange (ASCII) values into binary format and producing a moveof bits, binary conversion is carried out. In a similar fashion, in the cover photo, a byte stream is created from the bytes that represent the pixels. Message pieces are taken consecutively after whichare situated in LSB smidgen of picture byte. Until all of the message bits are located in photograph bytes, the same procedure is followed. Picture
produced is called 'Crypto-Picture'. It has been prepared for Internet transmission.

Cover image algorithm for concealing secret information:

- Step-1: Read the secret information that will be embedded in the cover image and the covermedia image.
- Step-2: Reduce the secret information.
- Step-3: Utilizing a secret key that is shared by both the sender and the recipient, convert the compressed secrets into ciphertext.
- Step-4: Convert a text message that has been compressed and encrypted into a binary format.
- Step-5: Determine the LSB value of each RGB pixel in the cover image.
- Step-6: Integrate the bits of the secret data into the cover image's bits of LSB and RGBpixels.
- Step-7: Keep going with the procedure until the cover document completely conceals thesecret information.

3.2. LSB Decoding

First, 'Crypto-Image' is taken and single array of bytes are generated as it become carried outat the time of encoding. The general number of bits of encrypted secret information and the bytes representing the pixels of Crypto-image are taken. Counter is to begin with set to 1,

which in turn offers the index range of the pixel byte where secret message bit is available in LSB. The procedure is continued till very last secret message bit is reached. After this, the bit circulationof the message shall be generated. Available bits are grouped to shape bytes such that each byte represents single ASCII character. Characters are stored in textual content record which represents the encrypted embedded message. After that the decryption and decompression are to be done.
Algorithm for un-hiding secret data from Crypto image:

- Step-1: Read the Crypto image.
- Step-2: Find LSBs value of each RGB pixel of the Crypto image.
- Step-3: Find and retrieve the LSBs of every RGB pixel of the Crypto image.
- Step-4: Continue the procedure till the message is absolutely extracted from Crypto image.
- Step-5: Decompress the extracted secret facts.
- Step-6: Using shared key, decrypt secret records to get original records.
- Step-7: Reconstruct the secret statistics.

3.3. XOR Encryption Algorithm

Although it is not a public-key system like RSA, exclusive-OR encryption is almost impossible to break using brute force. It is vulnerable to patterns, but this flaw can be fixed by compressing the file first (to get rid of patterns). Although the encryption algorithm is extremely straightforward and nearly impossible to break, exclusive-or encryption requires that both the encryptor and decryptor have access to the encryption key. The boolean algebra function exclusive- OR (XOR) is used to perform exclusive-OR encryption. XOR is a binary operator, which means it takes two arguments, much like the addition sign. By its name, exclusive-OR, it is clear that it will return true only if one of the two operators is true. This inference is correct.

Exclusive-OR encryption is based on the idea that without knowing the initial valueof one of the two arguments, it is impossible to reverse the operation. For instance, if you XOR two variables with unknown values, you cannot determine their values from the output. For instance, you cannot determine whether A is false and B is true or whether B is false and A is true if the operation A XOR B returns TRUE. Also, even if it returns FALSE, you can't be sure whether both were TRUEor FALSE.

Contrary to logical AND and logical OR, it is completely reversible if you know either A or

B. For selective Or on the other hand, on the off chance that you play out the activity A XOR Valid and it returns a worth of Genuine you know An is Misleading, and assuming it returns Bogus, you know An is valid. Exclusive-OR encryption is based on the idea that you can always decrypt correctly if you have the encryption key and the encrypted string. If you don't have the key, you can'tdecrypt it unless you make completely random keys and try each one until the decryption program produces text that can be read. The encryption key becomes harder to crack the longer you make it.

Taking the key and encrypting a file by repeatedly applying the key to successive segments of the file and storing the output is the actual application of exclusive-OR encryption. Because the key is generated at random, the output will be like a completely random program. The files can only be decrypted by someone with access to the key; without it, decryption is nearly impossible. The number of attempts required to break the encryption using bruteforce is doubled for each bit added to the key's length.

Exclusive-OR (XOR) encryption is a type of encryption that is difficult to crack using so- called "brute force" techniques. (Brute force means using random encryption keys in the hope of finding the right one.) However, pattern recognition is a possibility with the encryption method. Before the file is encrypted, patterns can be easily avoided by compressing it first (compression already renders it unreadable and removes patterns for you).

A public key, such as RSA, is not used in the XOR encryption method. Instead, the encryption key must be in the hands of both the people who encrypt the file and those who want to decrypt it. As the name suggests, the exclusive-OR encryption makes use of the Boolean algebra function XOR. Since it is a binary operator, the XOR function takes two arguments when used. Assuming that one of the two contentions is valid and the other contention is misleading, then, at thatpoint, the XOR capability will bring valid back.

IV. RESULTS AND DISCUSSION

Input Image Data Hidden within Text code

Text 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 upload medicaldata for transmit to the receiver. Medical data is present in the form of normal text in English words. Uploaded texts message was converted into TEXT format. TEXT is a quick response code that will be generated to provide secure to the medical data.

Image Upload

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 cryptography image that has to send should be uploaded. The image should be any one of the image supporting formats. The various supporting formats are JPEG, PNG & BMP. A text is written and hidden inside a secret image. This is done by using LSB method. The cover image is called as a steganographed image.

Image Encryption

Crypto image 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 TEXT code. By using this module, the encrypted image will be sent tothe receiver. This will helps to avoid the information missing and also it saves transmission and receiving time for both sender and receiver.

Image Decryption

The encrypted image 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 Crypto image in decrypted form. 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.

Recovered Text code and Medical Data

In this module receiver can retrieve Text code and text. After decryption image receiver can extract Text based text. Data extraction is the process of extracting the original data. The hidden text 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.

V. CONCLUSION

The proposed method explains how a secret image can be safely transferred from one location to another. The image that should be secretly sent to the recipient must be chosen by the sender. The secret image is divided into shares of number "n." The XOR operation encrypts each share. After that, the receiver receives all of the encrypted shares in a single transmission. The beneficiary ought to utilize the unscrambling key to decode the offers. The recovered (original) image will be created by joining the individual shares together following decryption. The size of the recovered image will be identical to that of the original. Because the confirmation is outfitted with the strategy's concept, it ensures that an adversary cannot alter the final picture without affecting the previous, making its security analysis simpler and more practical. The validation will be the focus of additional research in the future.

The recovered image size should be considered the same as the shared image in order to improve work authentication in the future. Encryption and decryption times for multiple shares can be calculated to improve performance, and noise should be reduced.

REFERENCES

[1]. Chen, Yu-Chi, Tsung-Hsuan Hung, Sung-Hsien Hsieh, and Chih-Wei Shiu. "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, Zhiyuan Yang, Yiu-Ming Cheung, Lingling Xu, and Shaohua Tang. "High- capacity reversible data hiding in encrypted images by bit plane partition and MSB prediction." IEEEAccess 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, 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.

[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 SignalProcessing (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, Yun-Qing Shi, Hong-Xia Wang, and Lin-Na 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.