Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

Data Hiding with Encrypted Multi Secret Sharing using Modified LSB Technique

A. Sendhooran
[1] Student,
Dept. of CSE Engg., Prist University, Thanjavur

Dr. R. Latha
[2] Associate Professor,
Dept. of CSE Engg., Prist University, Thanjavur

***Abstract*— Stegnography is a mechanism which ensures that the presence of the secret data remains undetected. Two types of secure data hiding techniques are popular, they are cryptography and steganography. Where cryptography is form of writing secret code for input message and steganography is art of hiding the secret message within cover file. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Steganography technique hides message into cover file and create a stego file. In image steganography there may be a need of technique which will helps to increase the security, reduce the distortion within the stego image and recovers the data without any loss. In the generation of multimedia and internet communication there may be need of lowering time for transmission. The major objective of this task is to establish a secured conversation among the sender and the receiver by using the use of 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. Modified LSB**
(Least Significant Bit) method is used for this purpose. Now the image is splitted into shares. Each share is encrypted using XOR method. The proposed technique is n out of n multi secret sharing scheme. Transmission of more secret images concurrently is achieved through 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.

Index Terms—Data Sharing, Multi Secret Sharing Scheme, Image Encryption, Data Embedding using Modified LSB, Key Verification, Data Retrieval.

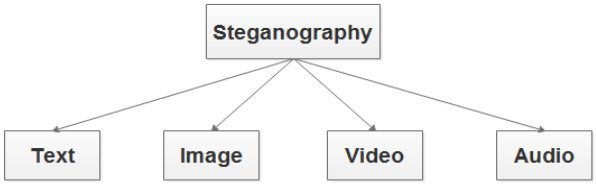
I. INTRODUCTION

STEGNOGRAPHY BASICS

Steganography replaces unneeded or unused bits in normal computer files (Graphics, sound, textual content) with bits of various and invisible information. Hidden data can be any other ordinary computer file or encrypted information. Steganography differs from cryptography in a way that it hides the message content wherein cryptography works to convert the content material of the message. Steganography from time to time used along with encryption. An encrypted file can also nevertheless hide information using steganography, so despite the fact that the encrypted file is deciphered, the hidden data isn't always visible. In modern-day times, this trouble may be observed in countrywide intelligence corporations attempting to locate public but covert communication among terrorists, or conversation between citizens in oppressive states that have outlawed cryptography.

TYPES OF STEGANOGRAPHY

There are exceptional approaches to cover the message in some other message, well known are Least Significant bytes and Injection. When a file or an image is created there are few bytes in the record or image which are not necessary or least important level. These sort of bytes may be changed with a message without adverse or changing the unique message, by means of which the secrete message is hidden inside the file or image. Another way is a message may be immediately injected right into a file or image. But in this way the size of the file could be increasing depending on the secrete message.



Stegnography in Image

Digital images are mostly used cover images for steganography process. Due to the availability of various file formats of different applications the algorithm used for these formats differs accordingly.

An image is collection of bytes (realize as pixels for images) containing exceptional light intensities in specific regions of the image. When managing digital images for use with Steganography, 8-bit and 24-bit in keeping with pixel image documents are typical. Both have benefits and demerits. 8-bit images format are mostly used because of their small length. The disadvantage is that only 256 viable colors can be used which can be a chance of problem throughout encoding. Usually a grey scale palette is used when dealing with eight-bit photos including (.GIF) because its slow trade in color would be more difficult to discover after the image has been

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

encoded with the secret message. 24-bit images provide a lot more flexibility when used for Steganography. The huge numbers of colors (over sixteen million) that may be used pass nicely beyond the human visual system (HVS), which makes it very difficult to come across as soon as a secret message has been encoded.

Large quantity of information can be encoded in to 24-bit image as its miles compared to 8-bit images. The disadvantage of 24-bit images is their length which may be very excessive and this makes them suspicious our internet due to their heavy length when in comparison to 8-bit images. Depending at the kind of message and type of the image different algorithms are used.

Techniques for Stegnography in Image

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

CRYPTOGRAPHY

Cryptography is the science of the usage of mathematics to encrypt and decrypt data. Cryptography enables users to manage sensitive information or transmit it throughout insecure networks (like the Internet) in order that it cannot be read by anyone except the intended recipient.

While cryptography is the technology of securing information, cryptanalysis is the technological know-how of analyzing and breaking secure communication. Practical cryptography system combines analytical reasoning, mathematical tools, sample finding, patience, willpower, and luck. Cryptanalysts are also referred to as attackers. Cryptology embraces each cryptography and cryptanalysis.

Cryptography is used in real time applications such as secure banking transactions cards, computer password protection and secure e- commerce transactions.
Three varieties of cryptographic techniques utilized in general.
1. Symmetric-key cryptography
2. Hash capabilities.
3. Public-key cryptography

MULTI SECRET SHARING

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into more than one portion referred to as shares so that qualified units of shares only employed to reconstruct the secret. Therefore the SS scheme is one of the maximum essential technologies to realize comfortable access manage. A typical example of secret sharing schemes is a (k, n)-threshold secret sharing scheme. In (k, n)-threshold based multi secret sharing schemes, a secret is splited and 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 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 the normal secret sharing schemes, secrets and shares are both visual information and their encryption and decryption is achieved with the aid of computer systems. The schemes encrypt a visible secret message into visible secret shares so that humans can recover the visible secret with their eyes by superposing a qualified set of visual shares printed on transparencies.

Data exchanged over the Internet is in the form of images, audio, video, text, handwritten text, graphic objects, animations etc... The media used in data exchange is unreliable and insecure. Security of the digital media has become an important topic as it can be copied and modified easily. Cryptography is one of the techniques, which can be used for provide security of exchanged data. It ciphers the plain text to make it as cipher text, which is actually communicated through the communication media so that intruders even if obtain the cipher text do not be able to decipher the original information hidden within the cipher text.

II. RELATED WORK

Jiantao Zhou, et.al,.[1] Proposed an encrypted RIDH scheme. The proposed method hiding a secret message with the usage of public key modulation technique and plays information extraction via providing the data distinguishability of encrypted and non-encrypted image blocks. The decoding of the message bits and the authentic cover file are blended together; this proposed data hiding approach belongs to the class of non-separable RIDH solutions. Compared with the unique unencrypted block, the pixels within the encrypted block tend to have a far greater uniform distribution. This motivates to introduce the neighborhood entropy into the characteristic vector to capture one of kind characteristics. Instead of thinking about normal encryption algorithms tailored to the scenario of encrypted-domain information hiding, here keep on with the conventional flow cipher carried out in the trendy format. That is, the ciphertext is generated through bitwise XORing the plaintext with the important thing circulation. The extensively used flow cipher AES inside the CTR mode (AES-CTR) is assumed. The resulting information hiding paradigm over encrypted domain may be more practically beneficial due to motives.

Monika Bartwal, et.al,.[2] In an image using the redundancy used a key of reversible data embedding for finding and embedding domain. To extend the alternative space the current strategies decrease the redundancy via the execution of pixel level calculation and employ image histogram. The current techniques show unlimited embedding quantity without seriously demeaning the visible excellence of embedded consequence. The first step is image division, the modern uncompressed image is separated into fragments A and B; and monitored through the LSBs. A is reversibly embedded into B, the usage of self-reversible placing and reversible information hiding approach. LSBs of A can be used to position up extra information. Afterward self

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

embedded information reorganized the image the usage of stream cipher. The values are 0 to 255 and signified by using eight bits. Afterward the encryption manner, the records hider positioned up the encoded image, and inserts a restrained data into it. The information hider can´t exchange the unique image and only can manage the access to the embedded information. The data mining and data extraction entirely differs from image decryption. Two exceptional cases are taking to expose.

Shuang Yi, et.al,.[3] Propose a new BBE algorithm for reversible data hiding in the encryption domain, which is totally different from traditional RDH methods. BBE can be utilized in different types of images such as binary, gray-scale, medical and cartoon images. Compared with existing state-of-the-art methods, it has significantly improved embedding capacity and quality of the marked decrypted image. BBE-RDHEI can also be simplified and utilized for binary images, while existing RDHEI methods are designed only for gray-scale images. To extensively improve the security degree of BBE-RDHEI, we additionally provides a protection key design mechanism such that BBE-RDHEI is capable of resist the differential attack, at the same time as current RDHEI techniques cannot. To enhance the robustness and performance of Reversible Data Hiding techniques in present noise and data loss attacks, here introduce a bit level scrambling system to BBE-RDHEI after secret data embedding to spread out embedded secret information over the complete marked encrypted image. As a result, BBE-RDHEI is able to recover most of secret data even if one bit-plane (e.g., LSB or MSB) of the marked encrypted image is completely removed. Moreover, any bit-stage scrambling algorithm may be used in our BBE-RDHEI. This is another level protection gain of BBE-RDHEI.

Xiaochun Cao, et.al,.[4] Proposed HC_SRDHEI method. For the content owner, the given cover image is represented in keeping with an over-whole dictionary via sparse coefficients. After that, for the given selected patches, the corresponding coefficients and reconstructed residual errors are encoded immediately without quantization. For most of the patches, the data size is well reduced in the basis of coefficient representation, thus the vacated room is preserved for high capacity data hiding after image encryption. Note that, for losslessly recovering the cover image, the residual errors are self-embedded into the non-selected patches. At the receiver side, when the receivers get encrypted image containing additional data, the processing steps depends on the role of receiver. If the receiver is a data hider and has the hiding key, he can extract the information without get knowledge about image content. If the receiver is an image owner and only has the encryption key, he can decrypt the image with a better quality. If the receiver is both the image owner and data hider, he has each of keys in such case. Thus, the data extraction and content material recovery are all completed, and both results are free of errors. At the end, for proposed framework, the data extraction and image recovery process are separable and reversible.

Kenta Kurihara, et.al,.[5] Perceptual image encryption is a processing technique which makes an image difficult to recognize visually. Number theory-based encryption methods, such as RSA, DES or AES are the most secure options. However, within the multimedia data sharing domain, many packages have sought a trade-off in security to permit different necessities, which include low processing needs, keeping bitstream compliance, and sign processing in the encryption domain, along with compression, watermarking, searching, and so forth. In this work, recognition on image compression structures in the encrypted area, particularly ETC structures, in which a content proprietor wants to securely transmit an image to a recipient, through untrusted channel provider. In particular, using the JPEG fashionable is meant as a compression approach. When a common key is used for all frames, the key management is simple because the number of keys is one totally. However, the difficulty to estimate the key decreases because each frame mutually has some correlation. On the other hand, when an individual key is applied to each frame, the estimation of the keys is more difficult. However, the key management becomes complicated due to a lot of keys. To overcome such situations, we propose a key management scheme the multidimensional hash chain. To overcome such situations, here advise a key control scheme the multidimensional hash chain. The proposed scheme divides a video sign into N periods wherein each period has T frames.

III. EXISTING METHODOLOGIES

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.

RHD-EI permits a server to embed extra message bits into an encrypted image uploaded by the content provider, and guarantees that the original content material may be losslessly recovered after decryption at 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. The scheme overview is described as follows. P will pre-process the cover-image and generate a new cover-image, referred to as the processed image, and then send H the encrypted image by using polynomial interpolation. H will obtain a new polynomial

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

which carries a secret message in the released LSB plane, and then use addition homomorphism to generate the encrypted image with embedded message. Finally, by decryption R is able to obtain the stego-image, and then recover the cover-image and secret message.

IV. SECURE DATA SHARING USING MULTI SECRET SHARING WITH ENCRYPTION APPROACH

The goal of this proposed work is to set up a secured communication among the sender and the receiver by using the usage of emails and other communicating modes. In this system, an XOR based multi secret sharing approach is proposed to share images from the sender to the receiver 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. Single transmission of multiple secret images 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.

METHODOLOGY

MPVD with LSB Algorithm

In the embedding procedure of a secret message, a cover image is partitioned into non-overlapping blocks of 9 consecutive pixels.

- A difference between pixels values are calculated the 9 pixels in every block.
- All possible distinction values are differentiated into a number of ranges.
- The calculated difference value then changed by using a new value to embed the cost of a sub-stream of the name of the secret message.
- The amount of bits which can be embedded in an image pixel pair is determined regarding the range of the difference value.

LSB Encoding

First the unique image and the compressed encrypted secret message are taken. Then the encrypted secret facts need to be transformed into binary format. Binary conversion is accomplished via taking the American Standard Code of Information Interchange (ASCII) values of the person and converting them into binary layout and producing move of bits. Similarly, in cover photo, bytes representing the pixels are taken in unmarried array and byte stream is generated. Message bits are taken sequentially after which are positioned in LSB little bit of image byte. Same process is followed till all the message bits are located in photograph bytes. Image generated is called 'Stego-Image'. It is prepared for transmission through the Internet.

Algorithm for hiding mystery facts in Cover image:

Step-1: Read the cover media image and secret information which is to be embedded in to the cover image.
Step-2: Compress the secret facts.
Step-3: Convert the compressed secrets into cipher textual content by way of using secret key shared through receiver and sender.
Step-4: Convert encrypted textual content message into binary codes for embedding process.
Step-5: Find LSBs value of each RGB pixels that present in cover image.
Step-6: Embed the bits of the secret data into bits of LSB of RGB pixels of the cover image.
Step-7: Continue the procedure till the secret information is absolutely hidden into cover document.

LSB Decoding

First, 'Stego-Image' is taken and single array of bytes are generated as it become carried out at the time of encoding. The general number of bits of encrypted secret information and the bytes representing the pixels of stego-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 circulation of 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 unhiding secret data from Stego image:

Step-1: Read the stego image.
Step-2: Find LSBs value of each RGB pixel of the stego image.
Step-3: Find and retrieve the LSBs of every RGB pixel of the stego image.
Step-4: Continue the system until the message is virtually extracted from stego 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.

XOR Encryption Algorithm

Exclusive-OR encryption, is not a public-key encryption algorithm such as RSA, is almost unbreakable through brute force techniques. It is at risk of patterns; however this weak spot can be avoided through first compressing the report. 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. Exclusive-OR encryption works by using the Boolean algebra function exclusive-OR (XOR). XOR is a binary operator (meaning that it takes arguments - similar to the addition sign, for instance). Exclusive-OR, it is easy to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

infer (effectively, no much less) that it will return true if one, and only one, of the two operators is true.

The idea behind exclusive-OR encryption is that it is impossible to reverse the operation without knowing the initial value of one of the two arguments. For example, if apply XOR of two variables of unknown values, no need to tell from the output what the values of those variables are. For instance, in case you take the operation A XOR B, and it returns TRUE, you cannot recognize whether A is FALSE and B is TRUE, or whether B is FALSE and A is TRUE.

Exclusive-OR (XOR) encryption is an encryption method that is hard to break through with "brute force" strategies (brute force = the usage of random encryption keys within the desire you discover an appropriate one.), however the encryption technique is prone to sample reputation. Patterns can be easily removed by compressing the file first (compression already makes it unreadable, it removes patterns for you) before it is encrypted.

The XOR encryption technique doesn't make use of a public-key, which include RSA. Instead both the people that encrypt the record as well as the people that need to decrypt the file need to have the encryption key. The X-OR encryption (as the name already tells you) uses the Boolean algebra function XOR. The XOR characteristic is a binary operator, this means that that it takes two arguments while create it. If one of the two arguments is proper and the alternative argument is fake, then the XOR function will return authentic.

PROCEDURE

Create Text Message

Secret Data hiding is a process of embedding the secret text message 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. Message text is present in the form of normal text in English words.

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. 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.

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. X-OR encryption method requires that both encryption and decryption process 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.

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.

Image Decryption

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.

Recovered Image and Text Extracting

In this module receiver can retrieve encrypted shares. After decryption image shares receiver can reconstruct the shares to get original cover image. Data extraction is the process of get the original data from cover file. 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.

MULTI SECRET SHARING FRAMEWORK

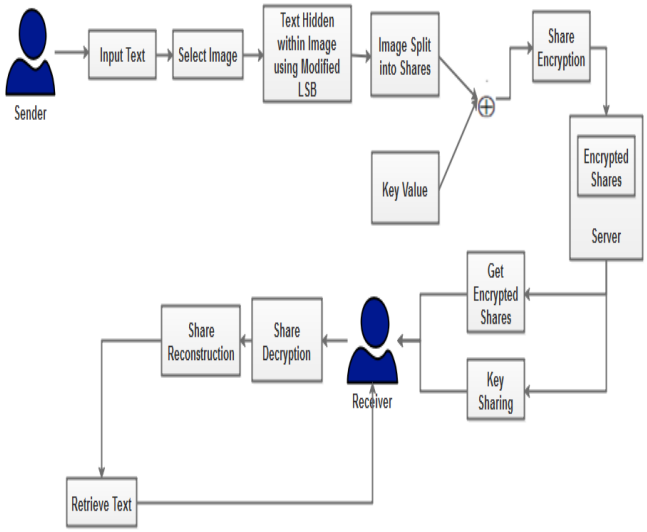


Fig 4.1: Architecture for Proposed Work

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 02, February-2021

V CONCLUSION

The proposed method describes the process of sharing a secret image securely 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 get decrypted image shares, the individual shares will be merged together to form the recovered (original) image. The recovered image will be of the same size as the original image.

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] 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.

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

[3] Chuman, Tatsuya, Kenta Iida, and Hitoshi Kiya. "Image manipulation on social media for encryption-then-compression systems." In 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 858-863. IEEE, 2017.

[4] 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.

[5] 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.

[6] 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.

[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] Kurihara, Kenta, Masanori Kikuchi, Shoko Imaizumi, Sayaka Shiota, and Hitoshi Kiya. "An encryption-then-compression system for jpeg/motion jpeg standard." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 98, no. 11 (2015): 2238-2245.

[9] 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.

[10] Xiang, Shijun, and Xinrong Luo. "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.

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

[12] 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.