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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

High-End Secure Image Transfer using Vector Quantization

B N V L S Kashyap
Department of. Computer Science and Engineering
Velagapudi Ramakrishna Siddhartha Engineering College
Vijayawada

N Y S Aditya
Department of. Computer Science and Engineering
Velagapudi Ramakrishna Siddhartha Engineering College
Vijayawada

K Pavan
Department of. Computer Science and Engineering
Velagapudi Ramakrishna Siddhartha Engineering College
Vijayawada

Dr. Ch Rupa
Professor
Department of Computer Science and Engineering
Velagapudi Ramakrishna Siddhartha
Engineering College Vijayawada,India

P Sahith Chand
Department of. Computer Science and Engineering
Velagapudi Ramakrishna Siddhartha Engineering College
Vijayawada

***Abstract*: While encrypting data is an explicitly affirmed requirement for many security-based services, the demand for more and more sophisticated and secure ways to store data is rapidly progressing. Images being a rich format of data are being demanded to have better encryption standards resulting in noiseless, visually compromising data. To address this problem, the project adopts an image encryption concept that embeds cipher images into the real data of the host image. A system is manifested through Data Hiding algorithms based on signal processing techniques like vector quantization. Thus, the original image is successfully encrypted and stegonized into the host image. This method of encryption strives at military, judicial, criminal record-based image data transfers where, though any unfortunate data leakages, the decrypting process gets more complex and the meaningful image might mislead the original content from being identified.**

Keywords: Steganography, data hiding, vector quantization, image encryption, secure transfer, secrecy communication.

I. INTRODUCTION

Encryption transforms the secrecy code from the normal plain text information which will be equaled to the original information. The process of encrypting the information comes under the property called cryptography. In information security, unencrypted data is also described as plaintext, and encrypted data is referred to be ciphertext. The steps and rules to be followed and used to encrypt, decrypt the messages are defined as encryption algorithms or ciphers. To be effective, an algorithm that consists of each and every part as a variable comes under cipher. Key is the derived word for the variable which makes a unique ciphers' output. When an encrypted message or the information is intercepted by an unauthorized entity, the intruder should unable to guess which cipher the sender used to encrypt the message, as well as what variables were referred to as keys. The longer time is taken for the intruder to guess this information is what makes encryption tougher and strengthener to such a valuable security tool. The essentiality of encryption defining the important content by means of securing and also to be protected from unauthorized access. The secrets of corporate companies are saved by these techniques protecting from other business organizations, the secure classified information, and processed information is used by the government also. Many individuals protect their personal information from theft by means of different encryption standards and security methods.

The following situation describes that a theft has happened and encrypted image was found by the hacker. To avoid this problem, it's better to have a highly encrypted image in the place of low-level encrypted image. A better technique is to separate the encrypted output with the noise. Hence, Reversible Data Hiding deals with a solution resulting in the image encryption with a meaningful noiseless output [14] and emerge for a secure transfer which can be defined in the paper.

The information and its security have a very big rise in each and every major research area under consideration. The size of data being processed has a very big growth rise and also it is a tedious process for handling them. Various methods are used for transmission of data in a secure way through the medium which is to be shared. One of those methods is hiding the data through cover media. The cover media page or the file may be of type text information, visual image, audio signals, or video transmission. The data (image and text) securing has increased widely in every requirement such as approaches like cover media using reversible data hiding technique which have been developed as an example for data securing methods using image transmissions. The method is reversible in nature as the original cover image can be recovered as such after the hidden message has been retrieved.

A non-separable method is the Reversible Data Hiding system which consists of an image and the data cannot be extracted independently which results in less flexibility. A new system

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

was proposed which was both separable and reversible in nature in order to overcome the limitations of the previous system.

The two main divisions defined as the content owner and the data hider in the Separable reversible data hiding. The original image was encrypted with a key for the former case while the latter exploits the spatial correlation to accommodate data of the original image and creates additional space. The receiver will unable to extract the original image having the data-hiding key even. Simultaneously, the receiver can extract the image with the encryption key, but not the data. He can extract the data as well as the original image content only if he has both the data-hiding and the encryption keys. For encrypting both the image as well as the data, the most incorporating efficient algorithms like AES which comes under the Separable reversible data hiding technique can also be used. In these criteria, the cover image is less prioritized when compared to information that is presented from the sender to the receiver used for embedding. The compression of the image and hiding of the data is done with the Lossy compression technique.

II. LITERATURE SURVEY

In [1], the paper describes the combination of both steganography with DCT and OTP encryption techniques. DCT ad OTP encryption describes that the watermarking [11] algorithm is based on it. The hiding of a secret message on an image with the DCT technique is used where the OTP encryption technique encrypts the secret message.

For applying the DCT technique, the cover image in the embedding process is divided into subdivisions. From each subdivision, the DC matrix is formed with the collection of DC coefficients. At the same time, the OTP encryption should be used to encrypt the secret message. The DC matrix got embedded and modified to form a cipher message. Inverse Direct Cosine Transformation (IDCT) is applied for the stego image to be produced.

Firstly, the cover image and stego image are partitioned into subdivisions in the extracting process and then the collection of their DC coefficients is formed from each subblock. The hidden message is extracted from the cover image and by using the OTP technique, the original message is obtained by comparing their coefficients.

In [2], the classification of data hiding techniques that can be used for hiding information in an image was discussed in this paper. Information can be embedded in an image in different ways is derived from these techniques (i.e.,) the cover image. It is embedded in such a way that the cover image is not distorted even after the message is embedded.

These techniques are referred to as spatial domain technique, transform domain technique, distortion domain technique, masking, and filtering. The important thing is to be noted that the data is hidden but not encrypted in the data hiding.

In [3], the paper mainly focuses on their level of applications on each of them by using different data hiding methods. Reversible data hiding says about previous works that are done before. Even though data hiding can be achieved through many methods that were explained, the limitations will be provided for each and every one of them. When reversible data hiding is applied on JPEG images because the compressed format of the original images is JPEG, therefore RDH cannot receive the compressed images and original images cannot be retained from them.

It is easy to hide the data in the Vacating Room Before Encryption (VRBE) method, such that in an encrypted image but is highly complex after the extraction of the data to retrieve the image from it.

In [4], to recover the original image from the stego image a novel that cannot be able without any distortion even after the message is extracted from the image reversible data hiding [8] algorithm is proposed.

The histogram of the image is explained by an embedding algorithm that uses to perform the embedding. Firstly, the histogram with zero points and peak points are identified as the embedding capacity which depends on the pixels that are associated with peak points in the histogram. The grayscale value in the range of 155 and 254 with the observation of complete image is for the pixels and based on the highest pixel value of the histogram it is shifted right. The process was programmed to be run several times until a proper output is obtained.

Similarly, an extraction algorithm is also explained which utilizes maximum point for extraction purpose and one minimum for an embedding algorithm. The algorithm is repeated multiple times for each pair until the multiple pairs are obtained. If any grayscale value is observed as an increment, the stego image is scanned and 1 is extracted otherwise 0 is extracted.

In [5], The Side Match Vector Quantization (SMVQ) technique was explained in this paper which discusses the scheme that is to be modified and used as a data hiding technique for which is low bit-rate compression. Generally, the images are compressed in SMVQ and the receivers are transmitted with indices values. The indices value will be changed when we try to hide data in it and results in the permanent distortion of the image which cannot be retrieved again. To avoid that problem, the modification of SMVQ technique is in such a way that directly the pixels values are transmitted which leaves the indices values same rather than transmitting the indices values to the receiver, it becomes easy to retrieve the image after the extraction of the data in it as before the data hiding takes place.

The reversibility ability consisting of the modified SMVQ technique without any distortion after the extraction process has through which the cover image can be obtained is done.

A preprocessing is to be done for this technique where all the data is to be transformed into digits beforehand. The compression of the secret message is to be done and embedded

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

without any problem before the embedding process. If the payload size is high, the stego image with a high level of distortion is obtained and vice versa as the distortion level depends on the payload size.

In any of the encryption techniques for security purpose, the secret message should be encrypted with as even as it shouldn't be understandable to the attacker even if the data is extracted from the stego image.

III. BASIC CONCEPTS

Steganography is covered through the transmitting method of data in a secret format so the very act of sending the data.

The contents of a cryptic message which is concealed were shown in cryptography, in which the transmission of a message is defined through Steganography. The concept has survived since biblical times but the notion of Steganography was first introduced earlier. In the Roman Empire, a worker was chosen to convey a secret message as there are tales of a method being used whereby a message was tattooed onto the skin, and the scalp was shaved clean. As soon as the hair grew up, he was forwarded on his mission to transmit the message. The receiver stripped the messenger's scalp over and understand the information. A kind of steganography techniques and algorithms have been accurately developed and tested. A summary of some of them is presented below.

The payload is encoded and transmitted in vector quantization steganography with one or several most limited significant bits of the carrier. The smaller the number of bits used to transmit the payload, the lower the impact on the original transmitter signal.

The JPEG-format transporters are very often utilized on Vector quantization steganography (i.e., when JPEG images are used to carry the payload). The transmitted information is secretly encoded into the coefficients in this method. With all other circumstances being equal, a slightly lower data-carrying function is found in this approach and provides one of the causes for this no data can be encoded whenever the coefficients take on these values such that the coefficient values of 0 and 1 cannot be altered.

The communicated data is encoded into most limited significant bits by using the vector quantization technique, the image palette willingly than into those of the carrier. The apparent utilization is a downside to its low data carrying capability feature.

The input formats consisting the use of service domains in which the payload is embedded into the service domains of the carrier's headers so-called as a comparatively manageable method. The low data-carrying ability was done by the downsides again and the embedded payload may be distinguished under payload protection that can seldom reveal the contents of the service domains routine using image viewing software.

The process of encoding the payload within the carrier is done with payload embedding and addressed which is decoded by using utilization algorithm which is known to both the individuals such as both sender and receiver. An autonomous encoding is done into the same carrier which is provided by various payloads which can be orthogonal by their embedding approaches.

Wideband arrangements happen into the subsequent types:

A secret carrier signal is accentuated by a pseudorandom signal which is derived through Pseudo random distribution method.

The frequency of the carrier signal switches according to a definite pseudorandom act which is defined as Frequency hopping classification.

Based on the experience of some information arrangements and including the data size in a header or the point that the handler of such formats holds the file till it transfers the end-of-data marker because the overlay picture of this is not decent steganography. The concatenating of an image file on the RAR/JPEG approach is an illustration that is familiar based on fashioned format division of a JPEG, followed by a RAR archive region. Scanning till the limits are specified in the file's header by the JPEG observer software program, while a RAR archiver appliance will neglect everything preceding to the RAR! The beginning of an archive is denoted by the signature. Disclosing the contents of the RAR archive so that the exposition of the image when it is opened in a RAR archiver is done if such a file is opened in an image file viewer. The carrier division should be superimposed as the downside to this approach which is added to the undoubtedly distinguished by an analyst visually examining the record.

Reconsidering the practices of concealing information in this section, we yearning only in image type carriers and network communication which are much wider for two areas in the utilization of steganography.

IV. PROPOSED METHODOLOGY

Architecture:

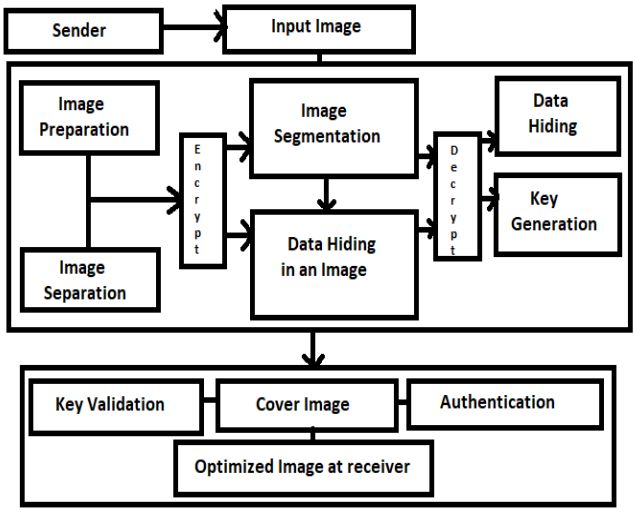

Figure 1: architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Encryption and decryption with the One-Time Pad:

The exclusive-or (XOR) performance is the very much used technique in encryption with the one-time pad [15]. The two indistinguishable bits were denoted by the exclusive-or such as (two zeros or two ones) which returns zero and a unit is represented as two disparate bits by the exclusive-or such as (a zero and a one). The code of the same length as information id encrypted which is confidence in one-time pad encryption. So, to convey the information in an encrypted way of one-megabyte to someone, you necessitate to securely partake one-megabyte information with the assigned receiver. Using the one-time pad encryption let us encrypt the information ENCRYPT for an instance. America Standard Code for Information Interchange (ASCII) protocol which is the standard practice of encoding letters in binary. The capital and lowercase letter and space encodings of each in binary are shown in Table 1.

In ASCII, ENCRYPT is encoded as
Text: ENCRYPT

E: 01000101
N: 01001110
C: 01000011
R: 01010010
Y: 01011001
P: 01010000
T: 01010100

Encoded: 01000101 01001110 01000011 01010010 01011001 01010000 01010100

Letter	Binary	Letter	Binary
a	01100001	A	01000001
b	01100010	B	01000010
c	01100011	C	01000011
d	01100100	D	01000100
e	01100101	E	01000101
f	01100110	F	01000110
g	01100111	G	01000111
h	01101000	H	01001000
i	01101001	I	01001001
j	01101010	J	01001010
k	01101011	K	01001011
l	01101100	L	01001100
m	01101101	M	01001101
n	01101110	N	01001110
o	01101111	O	01001111
p	01110000	P	01010000
q	01110001	Q	01010001
r	01110010	R	01010010
s	01110011	S	01010011
t	01110100	T	01010100
u	01110101	U	01010101
v	01110110	V	01010110
w	01110111	W	01010111
x	01111000	X	01011000
y	01111001	Y	01011001
z	01111010	Z	01011010
space	00100000		

Table 1: binary values

For the instance, we'll use the following as the one-time pad:
11010001 11000101 10010101 00101100 10111010 11101010 01101100

The exclusive-or of each bit of the message to encrypt the information using this pad is done with each bit of the one-time pad.

Plaintext: 01000101 01001110 01000011 01010010 01011001 01010000 01010100

OneTimePad: ^ 11010001 11000101 10010101 00101100 10111010 11101010 01101100

Ciphertext: 10010100 01001011 11010110 01111110 11100011 10111010 00111100

The decryption process to get the original message is similar to the encryption so that we can perform the one-time pad and exclusive-or of the ciphertext. This works because X^X = 0 (i.e. the exclusive-or of something with itself is 0).

Ciphertext: 10010100 01001011 11010110 01111110 11100011 10111010 00111100

OneTimePad: ^ 11010001 11000101 10010101 00101100 10111010 11101010 01101100

Plaintext: 01000101 01001110 01000011 01010010 01011001 01010000 01010100

Disadvantages of the One-Time Pad

Expecting a pad of the corresponding length with a one-time pad is the main drawback of encryption so that the information can be encrypted. The usage of considering each pad is only done once which signifies the corresponding length as the information to be yielded that it is essential to yielding a pad. The secure process of a pad must be accorded in a complete manner in order to safeguard the secrecy of the message. The presence of a secure practice that is accomplishing so in real-time the information could simply be sent is irrelevant since to accord the pad in this method.

Therefore, a huge quantity of the key substance in the use of exclusive consistency for a one-time pad has been accorded in progression which leads to pieces as messages are transmitted and then is followed up.

Advantages of the One-Time Pad

The one-time pad is random and only practiced once which is the principal benefit of the one-time pad encryption which is absolutely resistant. Each bit of the one-time pad is a one or a zero which is considered in a uniformly presumable so that a zero or one in the ciphertext has an equal possibility of obtaining a zero or one in the plaintext.

The most immeasurable cryptography protocols such as the one-time-pad is an example in which externally the benefit of a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

computer so that the work is done by hand. The pre-computer era was presented essentially and possession of a computer is prohibited is however beneficial in some situations or implicating or where the computers are not accessible.

The effective in positions of One-time pads where two individuals are in a secure situation need to communicate from two separate reliable situations and they oblige to withdraw from one another with comprehensive privacy.

Data hiding in still images

A category of difficulty that appears due to the access to the human visual system (HVS) in the still images of data hiding [10] proffers sculptures and images experience with the standard adjustments. Comparatively scanty host flag presented by still images to hide data as shown in Figure 2. A 200 * 200 pixels moderately conventional 8-bit image that affords roughly 40 kilobytes (kB) of input space in which to operate. Telephone-quality audio is commensurate to simply nearby 5seconds of or individual frame of NTSC television which are more limited. Moreover, still, images will be directed to services and prudent to suspect that extending from simplistic affine remodels to nonlinear transforms such as cropping, blurring, filtering, and lossy compression. As many of the transmutations are practicable so the Practical data-hiding procedures need to be repellent too.

Vector Quantization

For speech and image coding a lossy compression technique is used which is defined as Vector quantization [13]. Possible values are represented in a sample of scalar quantization, a scalar value is selected from a finite list. To represent an input vector of samples, a vector is selected from a finite list of possible vectors in the vector quantization. The quantization of a random vector by encoding the binary [12] codeword is the key operation in a vector quantization. In an n-dimensional space, each input vector can be viewed as a point. A partition of the space into a set of non-overlapping n-dimensional regions is derived from vector quantizer. Comparison of a codebook consisting of a set of stored reference vectors with the vector is encoded by a known code vectors which are optimality criterion so that consisting of all vectors that are closer to its code vector a quantization region should have any of the other code vectors, and the average of all vectors should be the code vector in the quantization region.

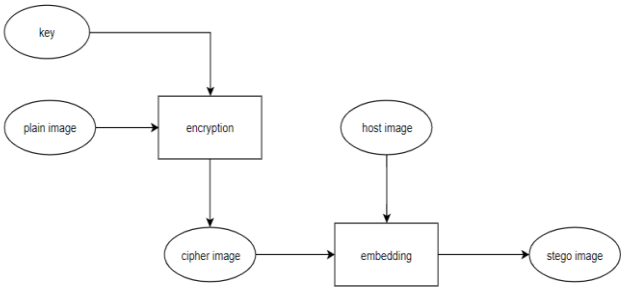

Figure 2: encryption and embedding

The figure 2 explains the encryption and embedding process [9] that takes place at the sender side resulting the stego image.

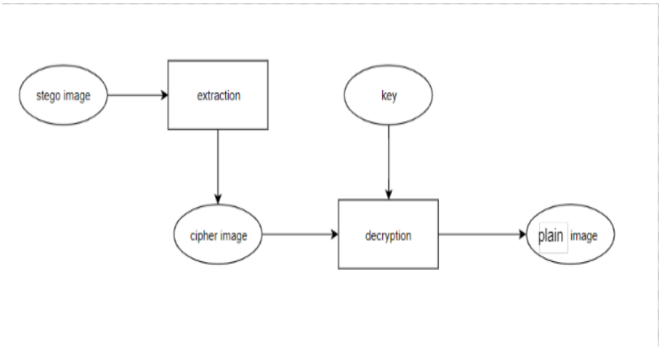

Figure 3: extraction and decryption

The figure 3 is the extraction and decryption process to obtain the original image from the stego image which is received from the sender.

V. IMPLEMENTATION AND RESULTS

Figure 4: plain image

Step 1: Image encryption

The image encryption [6] is done by using OTP (one time pad) encryption algorithm. A random key is generated every time when it is used.

Consider an image ‘pepper.png’ which is the image that is to be encrypted. Figure 4 shows the plain image to be encrypted. When the plain image (i.e) figure 4 is encrypted, encrypted image is obtained (i.e) figure 5.

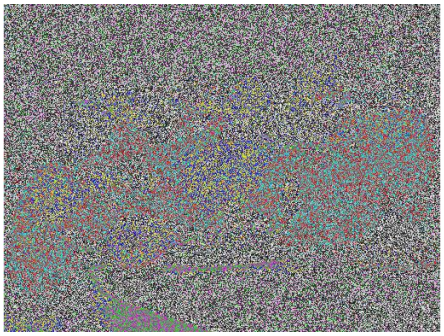

Figure 5: encrypted image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Step 2: Image embedding

In this step, a host image is considered, in which the image is to be embedded and transferred to the reciever. Consider an image 'bird.png' which is the host image (i.e) figure 6.

Figure 6: host image

The encrypted image (i.e) figure 5 is embedded into the host image (i.e) figure 6 by using vector quantization technique. When the embedding process is finished then the stego image is obtained (i.e) figure 7.

Figure 7: stego image

This stego image is transferred to the receiver while the attacker thinks the original content is 'bird.png' but not as 'pepper.png'.

Step 3: Image extraction

The reciever receives the stego image from the sender from which the original image is to be extracted. By using the vector quantization technique, the image is extracted from the stego image which is figure 8.

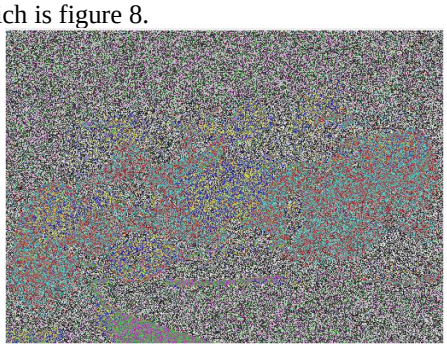

Figure 8: extracted image

Step 4: Image decryption

The image obtained after the extraction process (i.e) figure 8 is equivalent to the image that is embedded at the sender side. Key is generated at the reciever side and the the extracted image is decrypted by using the OTP decryption technique resulting the final output (i.e) figure 9.

Figure 9: decrypted image

VI. CONCLUSION AND FUTURE WORK

The most existing encryption algorithm was derived to address the security paleness of problems whose texture-like or noise-like encrypted images may lead to a large number of attacks and intruders to our system, this paper has introduced a new concept of image encryption to generate visually meaningful encrypted images that usually are considered as normal images rather than encrypted ones. The proposed concept ensures the attackers about the difficulty of correctly distinguishing with a large number of formats of encrypted images and locating the encrypted images from all normal images. Thus, with a much higher security level, the proposed concept can protect the original image compared with most existing encryption algorithms. The main idea is to embed a sparse representation of the host image into a secret image to achieve high secrecy. Our proposed algorithm has the following merits. In the Computer Security domain, A technique of Reversible Data Hiding [7] is proposed so that the data embedding capacity is deliberately higher than other similar schemes. In the reconstruction phase, We use matrix multiplication to decrease computational complexity. In the future, we aim to improve the strength of the proposed algorithm with lower computational complexity and to have the best secret communication through images from different regions.

VII. REFERENCES

[1] Rachmawanto, Eko Hari, and Christy Atika Sari. "Secure image steganography algorithm based on mean with otp encryption." Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493) Vol. 2 No. 1, April 2017, pp. 1 – 11

[2] Krishnapriya.K.R, ArunKumar.M.N, "Reversible Data Hiding In Image- A Literature Survey", International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017, ISSN No. 0976-5697.

[3] Raju, K. Upendra, and N. Amutha Prabha. "A review of reversible data hiding technique based on steganography." ARPN Journal of Engineering and Applied Sciences, VOL. 13, NO. 3, FEBRUARY 2018

[4] Ni, Zhicheng, et al. "Reversible data hiding." IEEE Transactions on circuits and systems for video technology 16.3 (2006): 354-362. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 16, NO. 3, MARCH 2006

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

[5] Chang, Chin-Chen, Wei-Liang Tai, and Min-Hui Lin. "A reversible data hiding scheme with modified side match vector quantization." 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers). Vol. 1. IEEE, 2005.

[6] Bao, Long, and Yicong Zhou. "Image encryption: Generating visually meaningful encrypted images " *Information Sciences* 324 (2015): 197-207.

[7] Sarkar, Tanmoy, and Sugata Sanyal. "Reversible and irreversible data hiding technique." *arXiv preprint arXiv:1405.2684* (2014).

[8] Megha Mohan, Anitha Sandeep. "Survey, Comparison and Discussion on Reversible Data Hiding Techniques" International Journal of Innovative Research in Computer and Communication Engineering, (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 9, September 2016.

[9] Wang, Ping, Xing He, Yushu Zhang, Wenying Wen, and Ming Li. "A robust and secure image sharing scheme with personal identity information embedded." *Computers & Security* 85 (2019): 107-121.

[10] Swanson, Mitchell D., Bin Zhu, and Ahmed H. Tewfik. "Robust data hiding for images." *1996 IEEE Digital Signal Processing Workshop Proceedings*. IEEE, 1996.

[11] Fu, Ming Sun, and Oscar C. Au. "Data hiding watermarking for halftone images." *IEEE Transactions on Image Processing*, Volume: 11, Issue: 4 , Apr 2002: 477-484.

[12] Wu, Min, and Bede Liu. "Data hiding in binary image for authentication and annotation." IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 6, NO. 4, AUGUST 2004: 528-538.

[13] Lu, Z.-M., Wang, J.-X., & Liu, B.-B. (2009). "An improved lossless data hiding scheme based on image VQ-index residual value coding". *Journal of Systems and Software, Volume 82, Issue 6, 1016–1024.*

[14] Li, Ming, et al. "Meaningful image encryption based on reversible data hiding in compressive sensing domain." *Security and Communication Networks* 2018 Volume 2018, Article ID 9803519 (2018).

[15] Horstmeyer, Roarke, et al. "Physical key-protected one-time pad." *Scientific reports* 3 (2013): 3543.