AN EFFICIENT MSB BIT PREDICTION USING CONVOLUTION NEURAL NETWORK (CNN)

Dr.R.Raju[1], Dr.A.Swaminathan[2]

#1 Professor and Head, Department of Information Technology, Sri Manakula Vinayagar Engineering College , Madagadipet, Puducherry.

 # 2 Assistant Professor, Department of Master of Computer Application , Sri Manakula Vinayagar Engineering College , Madagadipet, Puducherry.

Abstract:

Reversible data hiding in encrypted images (RDHEI) is a compelling procedure to insert information in the scrambled space. A unique picture is scrambled with a mystery key and during or after its transmission, it is conceivable to implant extra data in the encoded picture, without realizing the encryption key or the first substance of the picture. During the unraveling procedure, the mystery message can be removed and the first picture can be recreated. Over the most recent couple of years, RDHEI has begun to draw inquire about intrigue. In fact, with the advancement of distributed computing, information protection has become a main problem. Be that as it may, none of the current strategies permits us to shroud a lot of data in a reversible way. Right now, propose another reversible technique dependent on MSB (most huge piece) forecast with a high limit. We present two methodologies, these are: high capacity reversible data hiding approach with correction of prediction errors (CPE-HCRDH) and high capacity reversible data hiding approach with embedded prediction errors (EPE-HCRDH). Convolution Neural Network (CNN) models have been proposed and accomplished cutting edge exhibitions on identifying steganography

Keywords – MSB, CNN, Steganography.

I. INTRODUCTION

The computational analysis of objects in images is a very challenging issue as it usually involves automatic tasks for segmentation, that is, the detection of the objects represented, extraction of agent highlights from the items, coordinating between pictures, inflexible and non-unbending arrangement of pictures, transient following and movement examination of highlights in picture groupings, distortion estimation between two objects, as well as the 3D shape reconstruction of the objects from these images. Although, to carry out each of these tasks in a fully automatic, efficient and robust manner is generally demanding, some of these tasks often appear associated. For instance, to investigate the conduct of organs from successions of clinical pictures, first the info pictures ought to be fragmented, at that point reasonable highlights of the organs under examination ought to be extricated and followed along the picture arrangements lastly the movements included ought to be followed and broke down. The quality of the input images plays a crucial role in the success of any computational image analysis task, as the higher their quality is, the easier and simpler the task can be. Consequently, to improve the first nature of the information pictures, reasonable techniques for computational picture handling, for example, commotion expulsion, geometric revision, edges and difference upgrade and brightening remedy or homogenization, are required. Notwithstanding the inalienable troubles, computational techniques for picture handling and examination give a wide scope of significant applications for our general public. Applications regarding 2D, 3D or even 4D data can be easily found in surveillance, virtual reality, biomechanics, bioengineering and materials sciences. In this project, the computational methods of image processing and analysis that we have developed in order to analyze objects from images are introduced; particularly, those which have been utilized for picture division, coordinating, arrangement, following, just as for 3D shape recreation from pictures. Besides, their utilization in applications from medication and biomechanics to designing and materials sciences will be introduced and talked about. This project is organized as follows: in the next section, segmentation of objects in images is introduced with some of the methods that we have applied and some of their results. In the third part we talk about, the methods which we have been working on to match object nodes between images, to register objects in images as well as to estimate the deformation involved between two objects in images together with some of their experimental results. In the fourth section, the problem of tracking objects along image sequences is introduced showing some of our works in this domain and their respective results are presented. The 3D reconstruction of object shapes from 2D images is presented in the fifth section, along with some experimental results. Finally in the last section our conclusions.

II. MATERIAL AND METHOD

STEGANOGRAPHY

Steganography is originated from the Greek word, the word stegno means “covered” and therefore the word graphine means “writing”. The objective of steganography is to abstain from attracting doubt to the transmission of a concealed message. In the event that doubt is raised, at that point this objective is vanquished. Steganography could be a process during which a secret information is covered with images and therefore the message is decoded, when it reaches to the receiver .If anyone tries to look at the message he won’t see the covered data Steganography is employed within the corporate world to face corporate intelligence attempts. The terrorist organizations are using this steganography mainly to communicate secret information. The rumor is that some of terrorist organizations uses steganography by uploading the images on some websites and therefore the information is shared among them secretly. Steganography key schemes are been dependent on Kirchhoff’s principle. Steganography is the method of concealing private or delicate data inside something that seems, by all accounts, to be nothing out of the standard thing. Steganography is frequently mistaken for cryptology on the grounds that the two are comparative in the manner that the two of them are utilized to ensure significant data. One of the most broadly utilized applications is for supposed advanced watermarking. Media outlets is especially exceptionally apprehensive because of

the simplicity at which precise of computerized music and video can be made. A solution using steganography can be done by hiding notices or serial numbers or other copyright details inside the media. Steganography is an old technique that has existed since antiquity. Herodotus, a Greek historian who lived in the 5th century B.C., relates how the Greeks sent and received warnings of enemy movements using a message underneath the wax of a writing tablet. Steganography idea was first introduced by Johannes Trithemius in 1499 to share secret information for example hidden information was written on wood then information is covered with wax an unknown message was written on that wood ,invisible inks are also used in those days to implement Steganography. This steganography idea has been started in ancient Greece the same hidden idea is taking place in our modern days also to hide the secret information. In ancient ages the information is dependent upon the physical bodies (physical steganography) the medium used here are wood, skin, wax etc .This steganography method went on developing during the world wars to share the information more secretly a new carrier was introduced with electromagnetic waves at present digital images audio and video files are the most popular carriers .In a social relations exchange of information is involved which requires the protection so cryptography and steganography techniques came into pictures In steganography the sender and receiver are invisible , gives security as well as protection .steganography is the most productive method for Privacy and it is an apparatus for the cutting edge so File designs that are utilized to cover messages are Bmp,Jpeg,Gif.Wav,Mp3.

(a). Audio Steganography:

A steganography technique that uses audio because the cover media is termed an audio steganography. It's the foremost challenging task in steganography. This is often because the human sensor system (HAS) incorporates a larger dynamic range that it can listen over. Thus A steganography technique that uses audio because the cover media is termed an audio steganography. It's the foremost challenging task in steganography. This is often because the human sensory system (HAS) incorporates a large dynamic range that it can listen over. Thus, even a moment change in audio quality can also be detected by the human ears. Even a moment change in audio quality can also be detected by the human ear.

(b). Image Steganography:

A steganography technique that uses images because the cover media is named a picture steganography. Hiding secret messages in digital images is that the most generally used method because it can benefit of the limited power of the human sensory system (HVS) and also because images have an outsized amount of redundant information which will be won't to hide a secret message. To hide a message inside a picture without changing its visible properties, the quilt source will be altered in "noisy" areas with many color variations, so less attention are going to be drawn to the modifications. The foremost common methods to form these alterations involve the usage of the smallest amount significant bit or LSB, masking, filtering and transformations on the quilt image. These techniques will be used with varying degrees of success on differing kinds of image files.

(C). Encryption:

The process of converting the first message to cipher text is termed as encryption

(d).Decryption:

The process of converting the cipher text to plain text (or) original message is called as decryption.

(e). Steganalysis:

Steganalysis is an art and science of detecting message hidden by steganography, it's an analysation of recognizing pattern to check which format image belongs to the key issue for steganalysis is simply just like the patterns of recognition and have extraction. The features should show a discrepancy for the image without hidden image and for stego-image. The foremost notable steganalysis algorithm is that the RS attack which detects the stego-message by the statistical analysis of pixel values.

(f). Steganography Techniques:

Line shift coding, word shift coding, feature coding, Least Significant Bit insertion(LSB), Low Bit Encoding(LBE), Masking and filtering Steganography Usage in Modern Devices: for each page addition of yellow dots takes place, on these yellow dots time stamps and printed serial numbers are encoded as an example color laser printers

STEGANOGRAPHY CONCEPTS:

Multi-Level steganography (MLS):

Combination of at least two steganographic strategies prompts MLS .There are two techniques one is upper layer and the other is lower level upper level is a bearer for the another method that is a lower level, some of the interesting benefits to hide the information are binding the information into a file they are as follows Undetectability in upper level methods increases, total steganographic band width increases ,verification ability of steganogram integrity, steganogram extraction and analysation features a limit of successful identification. The concept of network steganography is extended and it is redefined for making it general few useful MLS applications are presented to improve secrete communications on telecommunication networks

SCTP STEGANOGRAPHY:

SCTP is a multi-spilling based technique, it is likewise one of the intraprotocal steganographic strategy the fundamental preferred position of this strategy is ensuing checksum will transmit in streams which are controlled by the bits of steganogram.

(a) Steganalysis meets cryptanalysis:

As we have seen right now the encrypted message are present in the source file (e.g. image)so to get the message we have to do cryptanalysis crypt algorithms are used for hiding the data. Hence it is required to recover the message

(b) Password guessing:

Try to get the password using social engineering technique and brute force attack.

(c). Stego-message:

The message after hiding into a desired file then the hidden message is called as stegano-message .

(d).Image Steganography:

Image steganography is one in all the steganographical method within which a secret message is hidden in picture which are uploaded on to online website and therefore the image will be uploaded directly to online websites and the image will be uploaded directly to online websites and the image will be downloaded by a particular person and the information will be shared among them secretly .Image file formats used to hide information are bmp, jpg.

DEEP LEARNING:

Higher layers might establish the ideas relevant to a personality's like digits or letters or faces. They sub-divide into several algorithms supports the coaching information set. Some well-liked example are: k-nearest neighbor line and logistical regression, SVMs, call trees and random forests, neural networks (RNN, CNN, and ANN), cluster (K-means, HCA).

CONVOLUTIONAL NEURAL NETWORK:

A convolutional neural system (CNN) is a particular kind of counterfeit neural system that utilizations perceptron's, an AI unit calculation, for administered learning, to dissect information. CNNs apply to picture handling, characteristic language preparing and different sorts of intellectual errands. Since the CNN takes a gander at pixels in setting, it can learn examples and questions and remembers them regardless of whether they are in various situations on the picture. Prior to the advancement of profound learning for PC vision, learning depended on the extraction of factors of premium, called highlights, yet these techniques need a ton of experience for picture preparing. The Convolutional Neural Networks (CNN), especially adjusted for picture preparing.

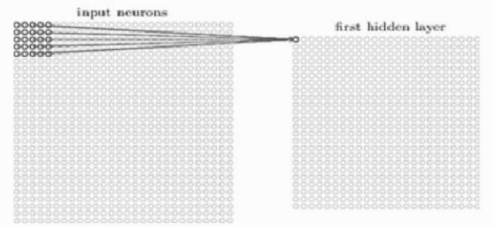

Fig 1. Gathering of inputs

A CNN is made out of an information layer. Be that as it may, for fundamental picture handling, this info is regularly a two-dimensional cluster of neurons which relate to the pixels of a picture. It likewise contains a yield layer which is ordinarily a one-dimensional arrangement of yield neurons. CNN, utilizes a blend of meagerly associated convolution layers, which perform picture preparing on their information sources. Likewise, they contain down examining layers called pooling layers to additionally lessen the quantity of neurons vital in ensuing layers of the system. Lastly, CNNs commonly contain at least one completely associated layers to interface our pooling layer to our yield layer, which are mentioned in the figure 2.

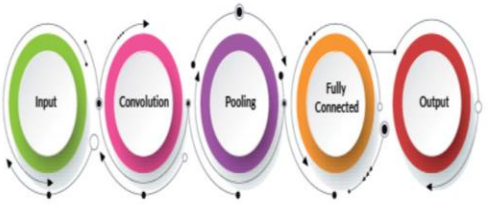

Fig 2. CNN LAYERS

Convolution is a system that permits us to separate visual highlights from a picture in little pieces. Every neuron in a convolution layer is answerable for a little bunch of neurons in the first layer. It contains channels or portion that decides the group of neurons. Channels numerically adjust the contribution of a convolution to assist it with distinguishing particular kinds of highlights in the picture. They can restore the unmodified picture, obscure the picture, hone the picture, and distinguish edges and so on. This is finished by duplicating the first picture esteems by a convolution framework. Pooling, otherwise called subsampling or down inspecting diminishes the quantity of neurons in the past convolution layer while as yet holding the most significant data. There are various sorts of pooling that can be performed. For instance, taking the normal of each information neuron, the total, or the most extreme worth. We can likewise switch this design to make what is known as a deconvolution neural system. These systems play out the reverse of a convolutional arrange for example As opposed to taking a picture and changing over it into a forecast esteem, these systems take an info worth and endeavor to create a picture. CNNs work well for a variety of tasks including image recognition, image processing, image segmentation, video analysis, and natural language processing.

III. PROPOSED SYSTEM

Image encryption algorithms and hiding algorithms should be designed to boost the effectiveness of transmission and keep safety from attacks by the intruders. The proposed method are able to do the information integrity, confidentiality and security. We are attempting to verify the confidentiality of gray scale image that creates uses of pixel shuffling and DWT stream cipher for cryptography and Hash-LSB, MSB for steganography. the most function of the pixel shuffling is that it involves no modification within the bit values and no expansion of pixels within the end of the encryption and also the decryption procedure. The pixel values are redesigned and combined moving from their particular positions so the values are swapped to offer the cipher image which becomes recognizable.

In additionally we are using SMTP protocol to induce the key image to the user and it will be retrieve by the password and it's randomly generated through the mail which it's safer. Every transformation of secret image, the password will be randomly generated by 4 bits. Through this password the key image can easily get by the user where the

information cannot be loss. It gives high quality of secret images and data to the user.

Convolution neural networks have shown to find out structures that correspond to logical features. These highlights increment their degree of deliberation as we go further into the network. Employing a Convolution Net will solve all the issues mentioned above. Firstly, the convolution net will have a decent idea about the patterns of natural images, and can be able to make decisions on which areas are redundant, and more pixels will be hidden there.

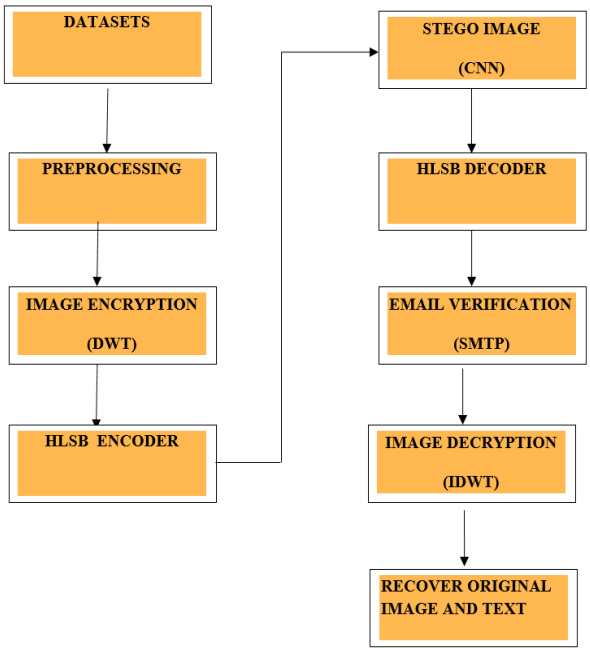

Fig 3. System Architecture

IV. IMPLEMENTATION

DWT ALGORITHM

A discrete wavelet transform (DWT) is any wavelet transform discretely inspected. Similarly as with other wavelet changes, a key preferred position it has over Fourier changes is transient goals. It catches both recurrence and area data (area in time).Wavelets are regularly used to denoise two dimensional signs, for example, pictures. Wavelets, in contrast, have both frequency and site. As in the past, the first finishes zero cycles, and the second finishes one cycle. Nonetheless, the third and forward both have a similar recurrence, twice that of the first. Instead of contrasting in recurrence, they vary in area — the third is nonzero over the initial two components, and the forward is nonzero throughout the second two components.

CONVOLUTIONAL NEURAL NETWORK

In this proposal, we present a practical embedded steganography scheme. Since JPEG images are widely used and pervasive, so we use them as cover. We use CNN because the target steganalyzer and therefore the baseline steganography scheme for conventional data embedding. The target steganalyzer is a CNN model composed of a fixed DWT filtering layer and 10 learnable convolutional layers. To the best of our knowledge, it achieves the best performance in detecting JPEG image steganography. In this proposal, we use JPEG cover images and stego images generated by CNN to train the target steganalyzer. However, other image formats, conventional embedding schemes steganalyzer, may also be applicable.

IMAGE TRANSFROMATION:

- By encoding and handling the picture data in quantum-mechanical frameworks, a system of quantum picture preparing is introduced, where an unadulterated quantum state encodes the picture data.
- To encode the pixel esteems in the likelihood amplitudes and the pixel positions in the computational premise states. Given a picture , where speaks to the pixel esteem at position with and , a vector with components can be framed by letting the principal components of be the primary segment of , the following components the subsequent section, and so on.
- A huge class of picture activities is straight, e.g., unitary transformation, convolutions, and direct separating. In the quantum processing, the straight change can be spoken to similarly as with the information picture state and the yield picture state .
- A unitary transformation can be actualized as a unitary advancement. Some essential and generally utilized picture changes (e.g., the Fourier, Hadamard, and Haar wavelet changes) can be communicated in the structure , with the subsequent picture and a line (segment) change grid .
- The comparing unitary administrator would then be able to be composed as . A few ordinarily utilized two-dimensional picture changes, for example, the Haar wavelet, Fourier, and Hadamard changes, are tentatively shown on a quantum PC, with exponential speedup over their old style partners.
- In expansion, a novel profoundly proficient quantum calculation is proposed and tentatively executed for identifying the limit between various districts of an image: It requires just one single-qubit door in the preparing stage, autonomous of the size of the image.

LSB &MSB:

- In computerized steganography, delicate messages might be hidden by controlling and putting away data at all critical bits of a picture or a sound record.
- In the setting of a picture, if a client were to control the last two bits of a shading in a pixel, the estimation of the shading would change all things considered / - 3 worth spots, which is probably going to be indistinct by the natural eye.
- The client may later recuperate this data by separating the least huge bits of the controlled pixels to recoup the first message.
- In registering, the most noteworthy piece (MSB, additionally called the high-request bit) is the bit position in a double number having the best worth.
- The MSB is now and again alluded to as the high-request bit or left-most piece because of the show in positional documentation of composing increasingly noteworthy digits further to
- The MSB can likewise relate to the sign piece of a marked twofold number in a couple of supplement

documentation, "1" which means negative and "0" which means positive.

WATERMARKING:

- A digital watermark is a sort of marker clandestinely implanted in a clamor open minded sign, for example, a sound, video or picture information.
- It is normally used to distinguish responsibility for copyright of such sign. "Watermarking" is the way toward concealing computerized data in a bearer signal.
- The shrouded data should, however doesn't have to, contain a connection to the transporter signal. Advanced watermarks might be utilized to confirm the realness or trustworthiness of the transporter signal or to show the personality of its proprietors.

V. RESULT AND DISCUSSION

The result/outcome of any image pre-processing method or technique is enhanced image with rich features in order to get the enhanced image a step by step procedure need to be followed where result of a step is feed as input to the next step for the feature extraction. From the actual/unique picture by expelling high power foundation clamor in the picture can be diminished in the mean while highlights with enormous contrast in the pixel force esteems are featured.. This processed image is converted to Grayscale image which gives the better visual information of a particular image. Both the statistical image data and processed images are trained with CNN models and the SMTP protocol to get the secret image to the user and it can be retrieve by the password and it is randomly generated through the mail which it is more secure. Every transformation of secret image, the password can be randomly generated by 4 bits. Through this password the secret image can easily get by the user where the data cannot be loss. It gives high quality of secret images and data to the user.

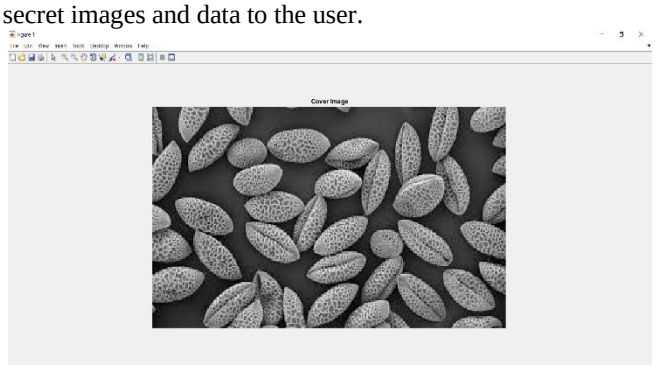

Fig 4.Cover image

Fig 5.Secret image

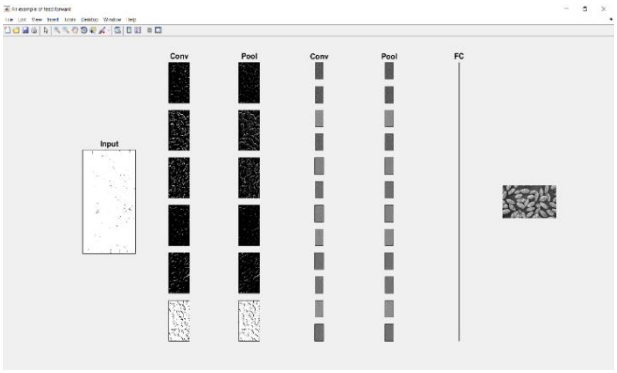

Fig 6.CNN layers images

Fig 7. Kernels of the Convolution layer 6

Fig 8. Kernels of the Convolution layer 6

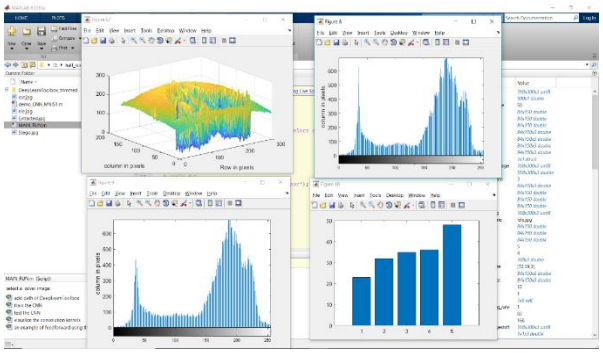

Fig 9. HISTOGRAM &GRAPH

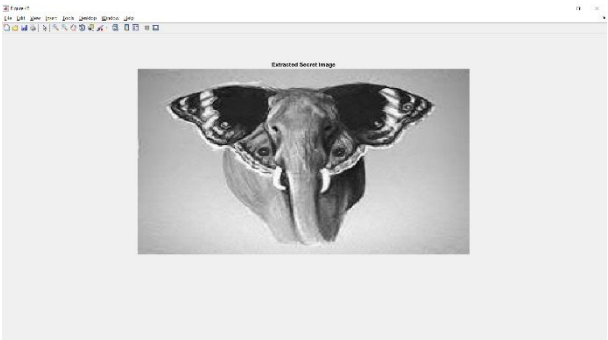

Fig 10. Extracted Secret Image

Convolution neural networks have shown to find out structures that correspond to logical features. These highlights increment their degree of deliberation as we go further into the network. Employing a Convolution Net will solve all the issues mentioned above. Firstly, the convolution net will have a decent idea about the patterns of natural images, and can be able to make decisions on which areas are redundant, and more pixels will be hidden there.

VI.CONCLUSION

The utilization of Secret picture serves the point of encryption, and DWT, watermarking, LSB and MSB calculation helps in improving the concealing limit the upside of utilizing DWT over different changes, is that it offers a fleeting goals. This algorithm is additionally stronger and robust likewise as secure compared to other algorithms. No visual defects will be observed from the corresponding stego images. It can even be observed devise new algorithms on ways to send different language secret texts or images in audio likewise as video files with more dynamicity. A quantum steganography method is proposed to cover a Quantum secret image into a Quantum cover image that's Quantum watermarking technique is employed to cover data. The proposed scheme utilizes the Arnold's cat map to form an incomprehensible watermark image before embedding it in an carrier image, then it's embedded by using Least significant bits.

REFERENCES

[1]W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2009, pp. 725 418– 725 418

[2] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," IEEE Transactions on Cybernetics, vol. 46, no. 5, pp. 1132– 1143, 2016.

[3] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP Journal on Information Security, vol. 2007, p. 17, 2007.

[4] X. Gao, L. An, Y. Yuan, D. Tao, and X. Li, "Lossless data embedding using generalized statistical quantity histogram," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, pp. 1061– 1070, 2011.

[5] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Processing Letters, vol. 19, no. 4, pp. 199–202, 2012.

[6]P. Puteaux, D. Trinel, and W. Puech, "High-capacity data hiding in encrypted images using MSB prediction," in Image Processing Theory Tools and Applications (IPTA), 2016 6th IEEE International Conference on, 2016

[7] Matthew Browne and Saeed Shiry Ghirdary," Convolutional Neural Networks for Image Processing:" An Application in Encrypted image,2012 IEEE International Conference on, 2012.

[8] Dan C. Ciresan, Ueli meier, Jonathan Masci, Luca M. Gambardella, Jurgen Schmidhuber," Flexible, High Performance Convolutional Neural Networks for Image Classification"

[9] Balaji.S,"Secure Data Transmission by The Steganography Using Private Key In Cloud ",International Journal of Pure and Applied Mathematics (IJPAM),Volume 119,Issue 14, 2018.

[10] C. Punithadevi, G. Shanmugasundaram, B. Thenmozhi, G. Raga, Kreethika Jain, "A Survey on Visual Cryptography Techniques used in Medical Images Encryption", International Journal of Computer Sciences and Engineering, Vol.7, Issue.3, pp.363-370, 2019.

[11] C.Punitha Devi, M.Subha, N.Danapaquiame, G.Siva Nageswara Rao, Pachipala Yellamma "The survey of an efficient search scheme over encrypted data on mobile cloud tees", International Journal of Pure and Applied Mathematics, VOL 117, No.19, pgs: 379-382, July 2017.

[12]M. Naor and A. Shamir, "Visual cryptography," in Workshop on the Theory and Application of of Cryptographic Techniques. Springer, 1994, pp. 1–12.

[13] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, pp. 354–362, 2006.

[14]"Separable reversible data hiding in encrypted image," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 826–832, 2012.

[15] X. Zhang, J. Long, Z. Wang, and H. Cheng, "Lossless and reversible data hiding in encrypted images with public-key cryptography," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 9, pp. 1622–1631, 2016.

[16] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 3, pp. 441–452, 2016.

[17]W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," in IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics, 2009, pp. 725418– 725418.

[18]P. Puteaux, D. Trinel, and W. Puech, "High-capacity data hiding in encrypted images using MSB prediction," in Image Processing Theory Tools and Applications (IPTA), 2016 6th IEEE International Conference on, 2016, pp. 1–6.

[19] Z. Qian and X. Zhang, “Reversible data hiding in encrypted images with distributed source encoding,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636–646, 2016.
[20]S. Jeong, C. Won, and R. Gray, “Image retrieval using color histograms generated by Gauss mixture vector quantization,” in Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 2004.
[21] G. Carneiro, A. B. Chan, P. J. Moreno, and N. Vasconcelos, “Supervised learning of semantic classes for image annotation and retrieval,” IEEE Trans. on Pattern Analysis and Machine Intelligence, 2007.