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

Dr.R.Raju
Dept. of Information Technology,
Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry
rajupdy@gmail.com

Dr.N.Arunachalam
Dept. of Information Technology,
Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry
narunachalam85@gmail.com

B.Rohenraj
Dept. of Information Technology,
Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry
rohanralph3@gmail.com

R.Gunaseelan
Dept. of Information Technology,
Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry
gunaseelan641999@gmail.com

A.Vijayarajh
Dept. of Information Technology,
Sri Manakula Vinayagar Engineering College, Madagadipet, Puducherry
vijayasai1973@gmail.com

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.

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 analisation 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:

Deep leaning could be a category of machine learning algorithms that uses multiple layer to more extract higher level option from the raw input, for instance, in image process, lower layers might establish the edges, whereas 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.

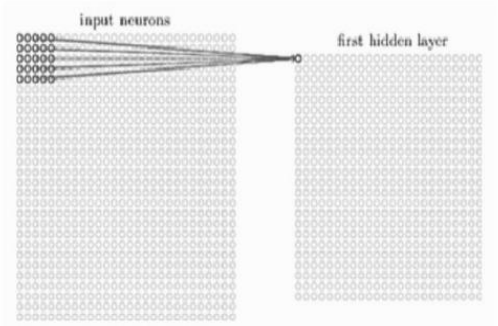

Figure 1: gathering of inputs

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.

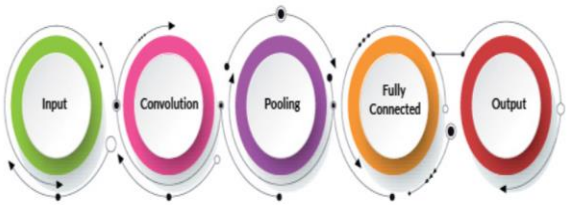

Figure 2: CNN LAYERS

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.

II.LITERATURE REVIEW

In literature survey, we learned a mechanism of steganography image and data encryption and decryption which protects data from the process. We analyze several literature surveys were the information was detected and the drawbacks which are occurred during the survey are totally changed and accomplished into a new technology based idea. We surveyed many ideas which were previous pre alarmed technology that were only based on algorithm. we produce a high efficient and high security gadget which are in high technology generation.

A. DATA HIDING IN ENCRYPTED IMAGE BYPATCH-LEVEL SPARSE REPRESENTATION [2][9]:

This project has proposed a novel method called the HC_SRDHEI, which inherits the merits of RRBE, and the separability property of RDH methods in encrypted images. Compared to state-of-the-art alternatives, the room vacated for data hiding by our method is much larger used. The data hider simply adopts the pixel replacement to substitute the available room with additional secret data. For this proposing they have proposed some modules which consist of encrypted image generation, data hiding in the encrypted image and data extraction and image recovery.

For simplicity, we use the grayscale images with 8 bits per pixel. The extension from gray images to color images is straight forward. For encrypted image generation, Given a cover image, we first divide it into patches that are then represented according to an over complete dictionary via sparse coding. Then, the smoother patches with lower residual errors are selected for room reserving. These selected patches are represented by the sparse coefficients, and the corresponding residual errors are encoded and reversibly embedded into the other non selected pathes with a standard RDH algorithm. At last, the room saved and self-inserted picture is encoded to produce the final variant.

Data hiding in the encrypted image, Once the encrypted image is received, the data hider can embed secret data for management or authentication requirement. The embedding process starts with locating the encrypted version of area A. Since the image owner has embedded the position of the first room preserving patch and the room size for each patch in the encrypted image, it is effortless for the data hider to know where and how many bits they can modify. After that, the data hider scans each selected patch in the encrypted image Ie, and simply makes use of bit replacement to substitute the corresponding bits reserved for secret data. Here, we assume the selected patch number is denoted as C, our MER for the data hider is computed as follows MER =C×8N2 −L(np nv)−nb−na N1 ×N2 where na is the dictionary size and is fixed for our algorithm. After data hiding, the position of the first data hiding patch and the hiding room size for each patch are also embedded into the encrypted image containing additional

embedded Note that, the mystery information is encoded by the information concealing key Kd before stowing away. Data extraction and image recovery, With the encrypted image containing additional embedded data, the receiver faces three situations depending on whether the receiver has data hiding and/or encryption keys. The data extraction and image decryption can be processed separately.

DRAWBACKS:

- The data hider simply adopts the pixel replacement to substitute the available room with additional secret data.
- The data extraction and cover image recovery are separable, and are free of any error.

B. ENABLING SEARCH OVER ENCRYPTED MULTIMEDIA DATABASE [1][10]:

This project makes the first endeavor on content-based retrieval over an encrypted multimedia database. Utilizing picture database for instance, we center around building secure search records, which shield the protection of picture content from the server and save the capacity of similitude examination. Two secure ordering plans, to be specific, secure transformed record and secure min-Hash outlines, are structured by mutually abusing systems from cryptography, picture handling, and data recovery. Both schemes can achieve good retrieval performance through encrypted indexes and serve as very good candidates for privacy-preserving multimedia retrieval. For proposing Encryption keeps data content safe from the server but also makes it difficult for the server to build searchable indexes.

In secure retrieval scenario, the search indexes need to be generated and properly encrypted by software tools on the user side using a secret key and then transferred to the serve. An desirable ordering plan for secure picture recovery, in addition to being efficient and versatile, ought to hold the likeness between picture matches and be appropriately made sure about utilizing a mystery key. Consequently, without knowing the key, it ought to be difficult to look through the database or induce data about the database content. Then again, the substance proprietor who realizes the mystery key can create an appropriately scrambled inquiry list from the question picture utilizing the mystery key. The server at that point contrasts the question record and the put away lists and returns the encoded files of the most comparable pictures to the client for decoding and review. The encoded question record additionally ensures the security of the inquiry picture.

An efficient method for speaking to pictures and conceivably empowering quick and adaptable inquiry is by the visual words portrayal .. Feature vectors are first extracted and hierarchically clustered into a vocabulary tree, and each image is then indexed based on this vocabulary tree and represented as a bag of visual words. This bag of visual words describes how many times the representative feature vectors in the vocabulary tree occur in the image of question, which is analogous to term frequencies in text retrieval and thus allows for extending the state-of-the-art text search techniques to images. The algorithm of min-wise independent permutation, known as min-Hash provides another efficient way to compare the Jaccard similarity between the visual words representations of two images. The min-Hash algorithm was originally developed to detect near duplicated copies of text documents; extensions to near duplicate detection of images have been proposed recently by applying min-Hash to the visual words representation. Here, we focus on the security aspect of the min-Hash algorithm and examine its performance for secure ranking of image similarity.

DRAWBACK:

- Improve the efficiency and security of search and retrieval, and change a lot of signal process within the encrypted domain to realize comprehensive secure data management.

C. LOSSLESS DATA EMBEDDING USING GENERALIZED STATISTICA QUANTITY HISTOGRAM [4]:

In this project, a generalized LDE framework was proposed by incorporating merits of the GSQH and the histogram-based embedding. In comparison with the existing LDE methods, the proposed one has better utilized the statistical characteristics of images and achieved better adaptability, flexible capacity control, and higher security. Thorough experimental studies show that this framework performs better than the conventional LDE methods based on the GH, and the method simply using the AADH.

Proposing system is for histogram-based LDE methods, the distribution of histogram has an important influence on the performance. In the proposed framework, a couple of histograms observing Laplacian-like distribution, including PEH, DH, and AADH, are contained in GSQH. The similar distributions can reduce the diversity of various images and guarantee the stability of the LDE methods. Among these SQHs, AADH is block based, which means the capacity can be adjusted flexibly [1]. Moreover, this blocking scheme can provide possibility for achieving robustness. Therefore, we focus on AADH and introduce the generation of it in detail. As known, the side information is important for the receiver side to extract the hidden messages, so it is valuable to store and transmit side information efficiently and safely.

In our framework, both the encryption and lossless compression techniques are adopted to solve this problem. On one hand, the location information of unavailable blocks, and several parameters, e.g., the scale factor and block size, are encrypted and transmitted to the receiver side via the ancillary channel. They served as a cryptographic key in the extraction process of the hidden messages. On the other hand, the location information of singular blocks is embedded into the host image as well as watermarks. To be specific, a flag matrix Mf, which indicates where the singular blocks are, is first compressed with a lossless compression algorithm, e.g., run length encoding (RLE). Following this, the compressed matrix Mc is concatenated with watermarks to form the final binary message stream BS, which will be embedded into the host image in the next subsection.

DRAWBACKS:

- Low limit particularly for the pictures with flat AADH.
- This system reacts to these issues by building the GSQH, using the scale factor for implanting zone determination, structuring the efficient techniques to deal with the overflow and sub-current

D. PROTECTION AND RETRIEVAL OF ENCRYPTED MULTIMEDIA CONTECT [11][3] :

The availability of signal processing algorithms that work directly on the encrypted data would be of great help for application scenarios where “valuable” signals must be produced, processed, or exchanged in digital format. In this project, we have broadly referred to this new class of signal processing techniques operating in the encrypted domain as signal processing in the encrypted domain. We mainly review the state of-the-art, describing the necessary properties of the cryptographic primitives and highlighting the limits of current solutions that have an impact on processing in the encrypted domain. Concerning the use of cryptographic primitives for signal processing in the encrypted domain, we can observe that treating the digital content as a binary data is not realistic and eliminates the possibility of further processing. Concerning the basic encryption primitives that make processing in the encrypted domain possible, for the particular case when it is necessary to compress an encrypted signal, a possibility is to resort to the theory of coding with side information; this primitive, however, seems to be applicable only to this kind of problem. In this proposal of the module the processing and encryption of multimedia content are generally considered sequential and independent operations.

In certain interactive media content handling situations, it is, nonetheless, attractive to complete preparing straightforwardly on encoded signals. The field of secure sign handling presents critical difficulties for both sign preparing and cryptography inquire about; just barely any all set completely

incorporated arrangements are accessible. This examination first succinctly abridges cryptographic natives utilized in quite a while to preparing of scrambled signals, and talks about ramifications of the security prerequisites on these arrangements. The investigation at that point keeps on depicting two areas in which secure sign handling has been responded to as a call, in particular, examination and recovery of mixed media content, also At last, the examination talks about the difficulties and open issues in the field of secure sign preparing.

DRAWBACK:

- In order to implement necessary signal processing operations, it seems crucial to have an algebraic cryptosystem.

E. HIGH-CAPACITY REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY BIT PLANE PARTITION [6][8]:

In this project, a replacement scheme for reversible data hiding in encrypted images has been proposed supported bit plane partition. The experimental results have shown that the more significant bit planes are suitable to be the quilt to cover the information within the less significant bit planes. After the method of self-embedding and vacating the embedded bit values, a substantial a part of the redundancy within the cover image may be preserved. Compared with the opposite schemes, the redundancy in plain-text images is best utilized with the proposed scheme because higher embedding capacity and better image quality may be simultaneously obtained. the preprocessed image is encrypted with a stream cipher by conducting exclusive OR (X-OR) operations, while the message to be hidden may be embedded in encrypted domain. By firstly extracting some auxiliary information from the encrypted image, the embedded data may be directly retrieved without image decryption. With the stream cipher utilized in encryption, the encrypted image may be decrypted to come up with a picture almost like the first one. After extracting the hidden bit values from the decrypted image, the first plain-text image may be recovered with the identical key utilized in self-embedding. the main points of every step within the proposed scheme are as follows image encryption, data embedding, data extraction, image decryption, original image recovery.

DRAWBACK:

- More complex.
- Less accuracy.
- Low PSNR and MSE.

F. CONVOLUTIONAL NEURAL NETWORK FOR IMAGE PROCESSING [7] :

Convolutional neural systems (CNNs) speak to an intriguing technique for versatile picture handling, and structure a connection between general feed-forward neural systems and versatile channels. Two dimensional CNNs are shaped by at least one layers of two dimensional channels, with conceivable non-direct initiation capacities and additionally down-testing. CNNs have key properties of interpretation invariance and spatially nearby associations (open fields). We present a portrayal of the convolutional organize design, and an application to pragmatic picture handling on a versatile robot. A CNN is utilized to distinguish and portray splits on a self-ruling sewer review robot. The channel sizes utilized in all cases were 4x4, with non-direct initiations between each layer. The quantity of highlight maps utilized in the three concealed layers was, from contribution to yield, 4, 4, 4. The system was prepared utilizing a dataset of 48x48 sub-areas drawn from 30 despite everything picture 320x240 pixel outlines tested from a prerecorded sewer pipe assessment video. 15 edges were utilized for preparing and 15 for approval of system execution. In spite of the fact that improvement of a CNN framework for common use is on-

going, the outcomes bolster the thought that information based versatile picture preparing techniques, for example, CNNs are valuable for picture handling, or different applications where the information exhibits are huge, and spatially/transiently dispersed. Further refinements of the CNN design, for example, the execution of detachable channels, or expansions to three dimensional (ie. video) preparing, are proposed.

G. FLEXIBLE, HIGH PERFORMANCE CONVOLUTIONAL NEURAL NETWORK FOR IMAGE CLASSIFICATION [8]:

We present a quick, completely parameterizable GPU usage of Convolutional Neural Network variations. Our component extractors are neither deliberately structured nor pre-wired, yet rather learned in a regulated way. Our profound various leveled models accomplish the best distributed outcomes on benchmarks for object arrangement (NORB, CIFAR10) and manually written digit acknowledgment (MNIST), with mistake paces of 2.53%, 19.51%, 0.35%, individually. Profound nets prepared by straightforward back-spread perform superior to progressively shallow ones. Learning is shockingly fast. NORB is totally prepared inside five ages. Test mistake rates on MNIST drop to 2.42%, 0.97% and 0.48% after 1, 3 and 17 ages, individually.

III.CONCLUSION

The motivation of this projects work is to implement image encryption, LSB and MSB algorithm helps in improving the hiding capacity. This algorithm is also stronger and robust as well as secure compared to other algorithms. No visual defects can be observed from the corresponding stego images. Convolution Neural Networks have shown to learn structures that correspond to logical features

REFERENCE:

[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.