Open Access Article

# AN EFFECTIVE SYSTEM FOR SECURITY OF SECRET INFORMATION THROUGH ANOMALY DETECTION IN REAL-TIME VIDEOS USING THE MATCH SUBSPACE SYSTEM AND THE STEGANOGRAPHY METHOD USING DEEP LEARNING AND CONVENTIONAL NEURAL NETWORKS

**Yelisela Rajesh[1] , Dr.Guruprakash.CD[2]**

[1] Research scholar, Dept. of CSE, Visvesvaraya Technological University, Belagavi.

[2] Professor,Dept.of CSE, SSIT, Maralur, Kunigul road, Karnataka.

Emails:[1] rajeshrajiv1324@gmail.com; [2] cdguruprakash@gmail.com.

**Abstract:**

Data security is critical. Cryptography and steganography are two of the most common security techniques. The hacker immediately identifies the secret information after following a few paths. This paper provides a new method for introducing secret data into a crowded scene using cryptography and the concept of image steganography, without employing the embedding notion. In this paper, firstly a novel supervised learning framework for detecting abnormalities in varied crowded scenarios is proposed. Visual features, motion features, and energy features are all available for busy settings. These characteristics are derived from spatiotemporal measurements. Three convolutional machines are trained for mid-level feature representation, and then a multimodal fusion model is used to deep understand the crowd patterns. One class support vector machine is used to track and detect abnormalities in a crowded scene based on the results of multimodal fusion. Apply the notion of deep conventional neural network to the image from the first step. Use one of the learned neural network techniques to map secret data into a vector. To obtain a stego image using this method, no mapping or embedding techniques are necessary. After the training phase, we utilize another neural network called an extractor to extract data from the stego image. We may also embed images into other images with two distinct networks using this technique. The secret image is embedded in the original image using the prep network. The hidden image is extracted from the stego image using the reveal network. This suggested technique was trained on a variety of data types and produced better outcomes in terms of embedding rate and extraction rate and payload capacity.

**Keywords:** Deep Learning, Feature Extraction, Multimodal Fusion, Anomalies, Support Vector Machines, Cryptography, Steganography, Deep Conventional Neural Networks

## I. Introduction:

One of the most important parameters in several sectors is data security. There are numerous approaches available to provide data security. One of the more conventional ways to data security is cryptography and steganography. Steganography is the process of concealing secret data in a carrier from unauthorized individuals. Text steganography, image steganography, and audio/video steganography are some of the approaches used. The secret data is hidden in text using text steganography. Secret data can be hidden or embedded in an image using image steganography. In

Received: February,03, 2023 / Revised: February,16, 2023 / Accepted: 25, February, 2023 / Published: 31, March, 2023

About the authors：Yelisela Rajesh

Corresponding author- Email:

general, data is available in a variety of formats, including text, image, audio, and video. This image steganography is usually carried out in two domains: spatial and transform.

Now a day surveillance videos are extremely in demand, and the demand is increasing day by day [1-4]. So many various applications are present for surveillance videos. One of the concentrated applications is anomaly detections. In general, the anomaly occurs at irregular events rarely for long time videos [7]. The detection of anomalies is one of the challenging tasks because the gathering of all anomalies from a single surveillance video is not possible and it is a desirable solution. To identify the anomalies one general and common solution is learning problems. With the help of learning problem, we learn the normal events based upon the training videos and identify, detect anomalies upon the distance of normal events and testing events [19].

Extracting numerous attributes for modelling video events is another duty for anomaly detection. There are numerous studies available for modelling films and finding distinct aspects from various views. In general, a histogram technique is used to extract low-level features [18]. Compute a histogram of gradient and optical flow to calculate the time for motion measurements using this method. Some existing algorithms extract trajectory-based information and apply the concept of semantic link between different objects [5].

In this proposed approach new novel multimodal representation was introduced to identify and detect anomalies for 3D images, and various complex crowed surveillance videos and images [15]. To identify a low level features this proposed framework consist of fusing multimodal approach with the help of spatiotemporal energy features. For this entire one, we proposed a new Deep Belief Networks (DBN) to achieve our goals. The main objectives of this proposed approach includes

- To gain various middle-level features, a new supervised deep learning model is used.
- A new multimodal fusion method is developed to discover high-level features for simulating a variety of crowded occurrences.
- A new way of leveraging deep conventional neural networks is employed to detect abnormalities in crowded photos or videos using the Match Subspace System (MSS) and one class Support Vector Machine (SVM). This technique differs from previously used methods such as the LSB embedding process and the DCT coefficients embedding programme. We employ a neural network to build a cover image based on the secret data in this way.
- We utilize a highly trained network and extractor to extract data from the stego image.
- We can integrate the image into another cover image with minimal noise in this proposed direct.

The remainder of the paper is laid out as follows: Section II contains a collection of existing image steganography and anomaly detection algorithms. The proposed technique is presented in Section III. Section IV contains the results and their analysis in relation to various steganography parameters. This suggested work's conclusion and future scope are presented in Section V.

## II. Related Works:

Various Existing algorithms are presented to identify anomalies in 3D images and videos. All of the existing work is broadly classified into two types. Those are trajectory-based methods and

spatiotemporal patch-based methods [6]. In general trajectory-based methods have different steps [7]. In the first step, we extract various features to model the normal events. Secondly, perform trajectory clustering operation for features representation to modal the normal events [8].

Pici et al. [9]proposed a new algorithm for anomaly detection for 2D and 3D images. In these similar features are formed as a single class cluster and then apply one class Support Vector Machine to identify and detect anomalies in an image. Cuirealli et al. [10] introduced a new algorithm based on the interaction energy. Bera et al. [11]proposed a new algorithm for addressing segmentation problems. Wu[16] proposed a new algorithm based on the correlation dimensions. Adam Proposed an approach based on the histogram of optical flow regions with the help of distribution concept. Mehrand [12] proposed a general social model to identify and analyze the behavior of the image like crowd behavior. Man[17] proposed combinations of various component analyzers to identify and model the events.

Lucak [13] proposed a new algorithm to identify gradient features for 3D images. It uses high-speed learning framework for model normal/abnormal events. These model detect anomalies with 150 frames per second. The speed of this one is one of the best one with compare to various existing algorithms. Lipi [14] developed a new hierarchical dynamical texture model of the video, based on the temporal model and spatial model.

Wang [21] had proposed a new algorithm based on the real-time camera position. In this technique first, extract the reduced features from the input or surveillance image and then identifying the anomaly detection based on the features extraction and motion of the camera. In general, if the motion of the camera was changed it leads to change in the features of the image. False alarms are obtained due to noise in this algorithm the noise ratio was gradually less. In some of the techniques, anomaly detection was divided into two different types, i.e. event encoding and anomaly event detection model based on these two models this model presents different techniques hidden methods such as Markova models [22]. In order to test the anomaly detection in images, videos and audio a new type of dataset was proposed, i.e. Street Scene. It consists of more accurate and high pixels image and videos. The noisy percentage of the video was minimum when compared to other data sets [23].

Zhu [24] had proposed a new algorithm based on the context information. Completely it is a mathematical model used for detecting the anomalies of a 3D image. In this we consider the activities which are occurred from the space and those are treated as features for extraction.

Milmamal [4] presented an LSB method upgrade. Insert the secret info into invertible pixels of the original cover image using this technique. When compared to many other LSB-based algorithms in spatial contexts, this approach has a large payload capacity and takes a long time to embed data.

Based on the LSB non sequential embedding, Rich et al [7] proposed the most reliable and accurate approach for embedding secret data. Another method for adding secure information into an image was proposed by Shital et al [8]. This proposed technique works best with JPEG images. To obtain stego analysis features, a Markov process was used. Fridrich [9] proposed a method that uses a Markov process and a discrete cosine transformation. To extract features from a JPEG image, both techniques are used. Pevyes et al. [10] developed a SPAM for calculating features for steg analysis of stego images

in a spatial domain setting. To extract more characteristics, utilise the markov technique to determine the difference between neighbouring pixels.

Based on the cover synthesis, Otori[15] presented a novel technique. The texture synthesis transformation methods described by Xz et al [16] were unique. It's used to convert a stego image from an input image or text. The stego texture is generated with the aid of mathematical functions based on the real-time synthesis system, and the concealed data is recovered with the help of the decrypter function [23].

## III. Proposed Model:

The structure for the first phase of proposed model is shown in Fig. 1

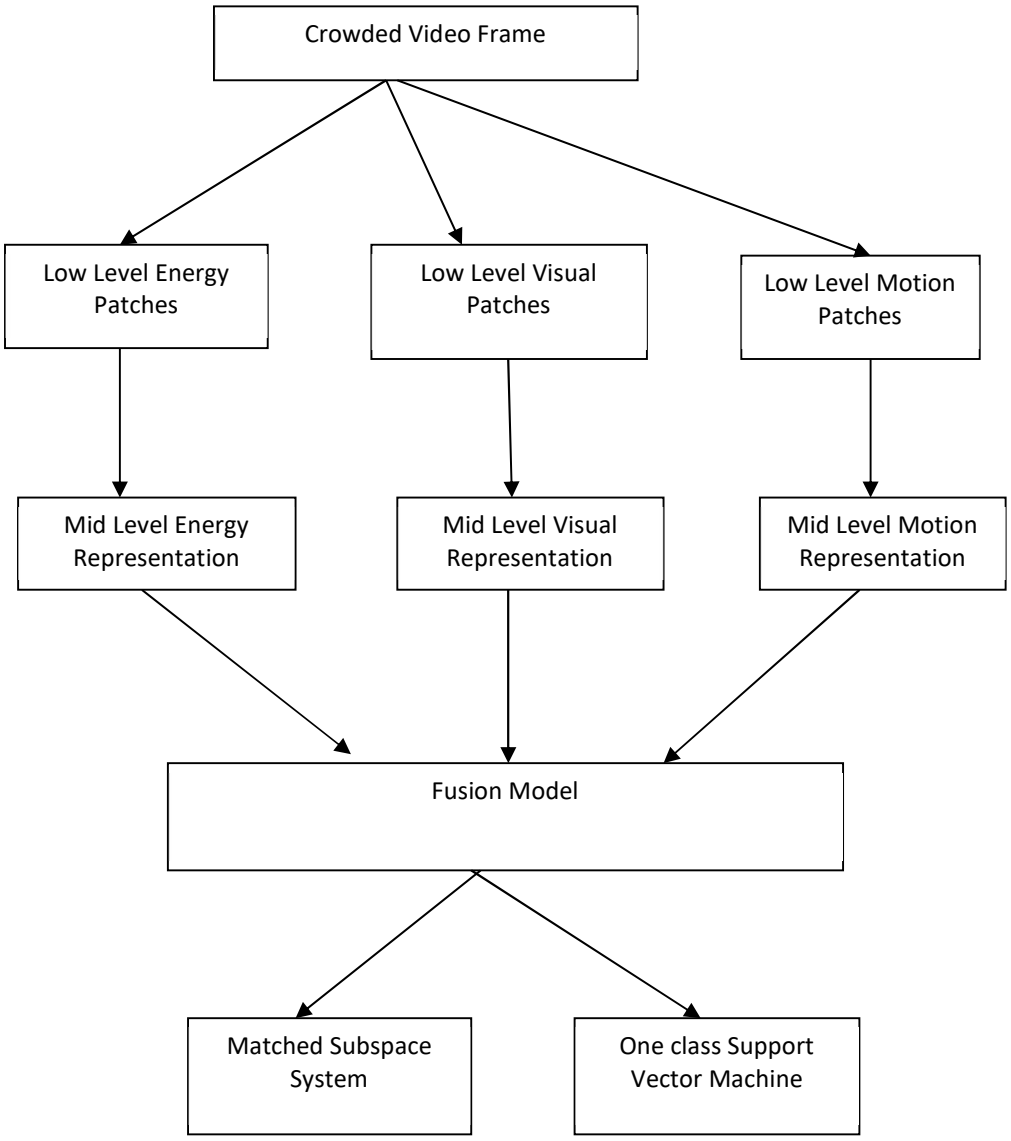



Fig.1. Phase I structure for the proposed model

To train and learn deep representations for images, one of the available algorithms, the Conventional Restricted Boltzmann Machine (CRBM)[16], is utilized. There are two layers: the input layer and the hidden layer. Binary values of visible units make up the input layer. The internal concealed layer is made up of two layers: a detecting layer and a pooling layer. N groupings of units make up each tier. Each detection layer group contains Kh×Kh array units, while each pooling layer group contains Kp×Kp units of p. B*B blocks were used to split the detecting layer. These are linked to a single pa pooling layer. The following is the energy function for CRBM.

$$E(v,h) = -\sum\sum i,j\ (hi,jk(Z\tilde{}\times v)i,j + Cktijk) - a\sum i,j\ vi,j \qquad (1)$$

Where Ck is the detection layer's shared bits, and h is the weight for vertical and horizontal matrix flipping.

DBN is generated by employing CRBM to learn mid-level features. Low-level motion features are represented using the primary spatiotemporal energy. X=(x, y, t) is the energy at each pixel, which may be determined using 3D Gaussian filters

$$St0\theta(x) = \Sigma x£\Omega(G\theta3 \times V) \qquad (2)$$

Where Gθ3 is the Gaussian filter and V is the Input Video

**Multiscale Motion Mapping with Deep Belief Networks:**

By considering three different patches in Fig 2. In this, the walking man present with a high speed in red patch, normal speed in the blue patch and green patch contain learning post. Fig 3 (a) to Fig 3 (c) shows energy distribution for different patches.

In this, we proposed multiscale energy for mapping different energy speeds. In this binary image is taken into consideration, three scale energy maps are used to map different energy where each of the channels is mapped with a binary image of the same size. In this two different threshold values like T1 and T2 always choose the channel whose threshold value is T1<T2. If the mean threshold value is less than T1, then patch 1 foreground pixels are changed to 1 otherwise the current patch or second patch values are held based on the threshold value of the second patch.

Fig. 2. Crowded Frame

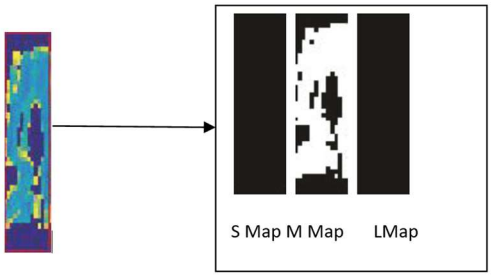



Fig 3(a). Energy of Green Patch

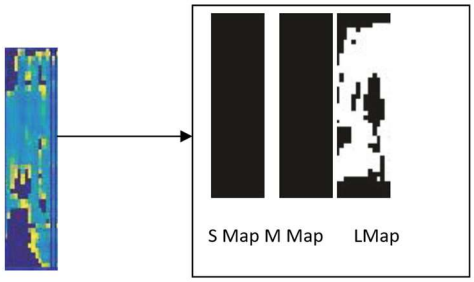



Fig 3(b). Energy of Red Patch

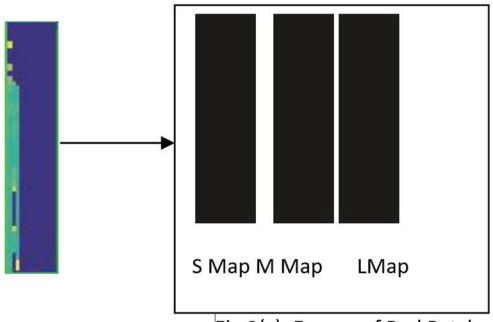



Fig 3(c). Energy of Red Patch

**Identifying high-level features with a fusion model framework**

The current framework consists of two steps

1. Training of deep belief networks with motion map and obtain features from the trained crowd video
2. Learn the correlation between middle-level features

To train the network use a supervised learning algorithm in layer by layer bit one layer at a time. After training the first layer the parameter of first layer w1, b1 and b0 are frozen, and hidden value h1 of the first layer is inference. The hidden values serve as input for the next layer[17]. The proposed model uses a directed graphical model with reasonable binary units. The energy for them is defined as

$$E(h12, h12v, h1\ 2map, h3\ , \theta) = \Sigma\ F\ i = 0\ b1i2h1i2 + \Sigma\ F\ i = 0\ b1i2v\ h1i2v + \Sigma\ F\ i = 0\ b1i2map\ h1i2map \quad (3)$$

Where θ is the model parameter and h3 is a bias of the hidden layer. The following formula gives the distribution of the three different set of visible and hidden layers units.

$$P\ (h1k2 = 0|h3) = \sigma(b1k + \Sigma\ F\ i = 0 Wkih1i3) \quad (4)$$

$$P\,(h1k2v = 0|h3) = \sigma\,(b1k2v + \Sigma\, F\, i = 0Wki3vh1i3) \quad (5)$$

$$P\,(h1k2map = 0|h3) = \sigma\,(b1k2map + \Sigma\, F\, i = 0Wki3maph1i3) \quad (6)$$

Where σ is the sigmoid function

In this, we have two different concepts

1. Anomalies detection with Match subspace System
2. Anomalies detection with one class support Vector Machines

Anomalies detection with Match Subspace System: A separate MSS is used for each layer because we deal with 3D image and the anomalies also in Nn×Nm spatial size. In general for detecting of subspace signal use Gaussian formulas here, we use matched subspace detector for detection of signals in subspace.

Let Xl represents layers L and XL(s) represents pixel at Xl for each pixel we create row stacking and column vector. For this, we define two hypothesis values those are

Let m1(s) be a vector of size Nn×Nm and ϕ1(s), and θ(s) be the weight vectors.

H0=S1 ϕ1(s)+m1(s) (7)

H1=H1 θ1(s)+ S1 ϕ1(s)+m1(s) (8)

H0= ϕ1(s)=P0∑vi-1/2n1(s) (9)

H1=P1∑vi-1/2n1(s) (10)

Where P0=(SiT∑vi-1S1)-1SLT∑vi-1/2 (11)

P1=(SiT∑vi-1S1)-1SLT∑vi-1/2[S1H1] (12)

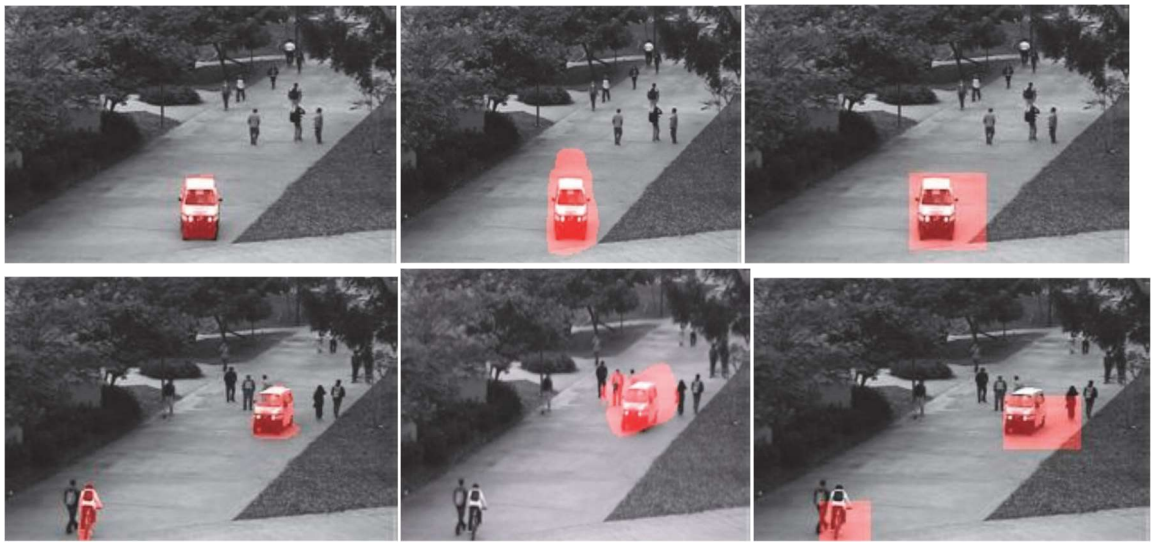
The decision is framed by either P0 or P1

Anomalies detection with one class support Vector Machines:

One class support vector machine is used to detect anomalies in crowded video the one SVM problem can be identified using the following formula.

Min a,b,c ‖a‖/2-C+1/nN∑i=1Nbi (13)

Where a is learning weight vector and c is offset. N is the size of the dataset b is the slack variable for patch i. The Comparison of anomaly detection of the proposed method with MST is shown in Fig 4



a. Ground Truth b. MST c. Proposed Method

Fig 4: Examples of abnormal detection on the data set

**PHASE II PROPOSED METHOD:**

**CASE I:**

There are two steps in the process of creating a cover image. Divide the original secret data into an equal number of segments in the first phase. Each data segment is represented as DS, and the noise vector Yi is mapped onto each data segment. Obtain the cover image in the second phase. Because this technique does not have an embedding step, the cover image is a stego image. Several bits of data segments are mapped with the noise vector ratio in this mapping process. The random function is used to produce those values.

$$r=random(x/2^{\sigma}\text{-}1+S\ x+1/2^{\sigma}\text{-}1\text{-}1\text{-}S) \qquad (14)$$

Where the random function is use to generate the random values for the noise function. The noise vector values are in the range of $(x/2^{\sigma}\text{-}1\text{-}1,\ x+1/2^{\sigma}\text{-}1\text{-}1)$. Where $^{\sigma}$ is the $DSi/Y_i$. The diagram representation of the phase I process and the mapping process is shown in Figures 5 and 6.

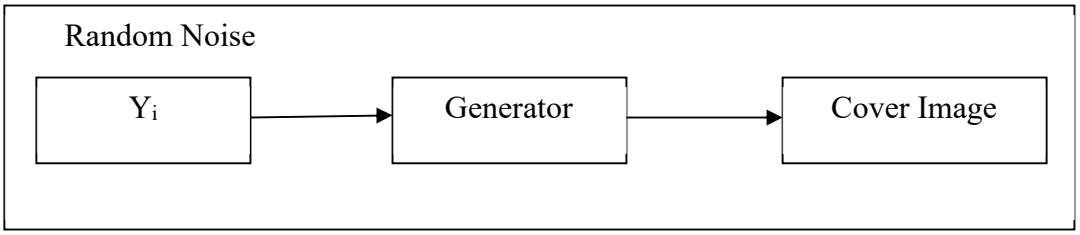



**Figure 2: Generating Cover Image Process**

**Fig 5.Generating Cover image**

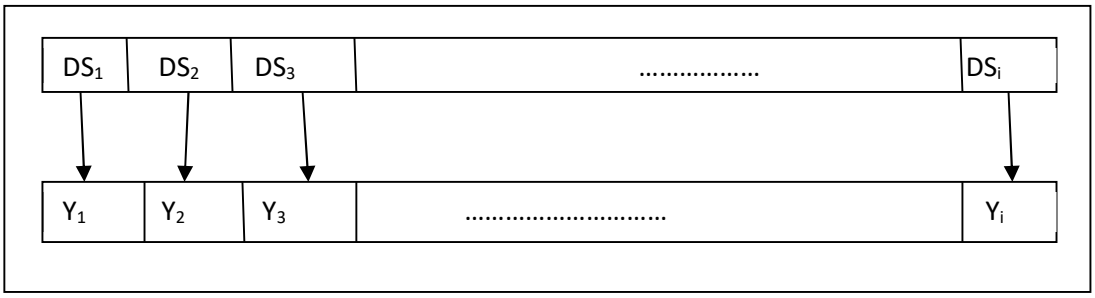


**Fig 6: Mapping process Data Segments and Noise Vector**

**Algorithm I:** Generating original cover image

Input Variables: Y,X,σ

Output: Stego Image

1. Obtain the generator by using equation 1
2. t=c*X
3. n=length(Y)/t
4. Divide the secret data into nu number of segments of its length t
5. for k=1 to n do
6. for w=1 to t do
7. a=0
8. for z=w to w+ σ -1 do
9. $a=a+2^{w+\sigma-1-zY_{ij}}$
10. end for

**Case II:**

In this phase design conventional neural network called as a extractor, used to recover or extract data from the stego image. This conventional neural network is obtained in the form of layers. Each layer is interconnected each other with another layer. The structure of layered organization is shown in Fig 7.

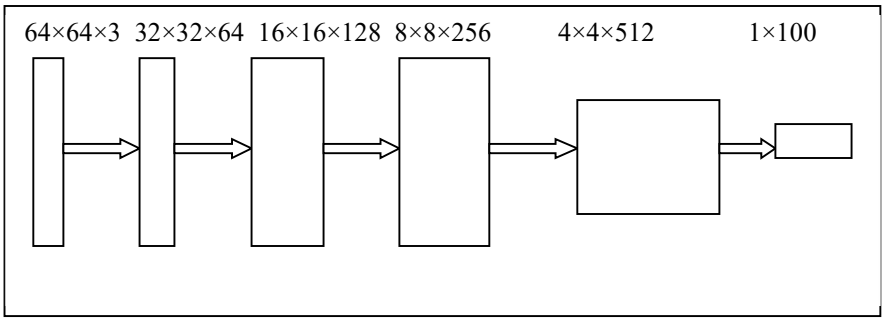
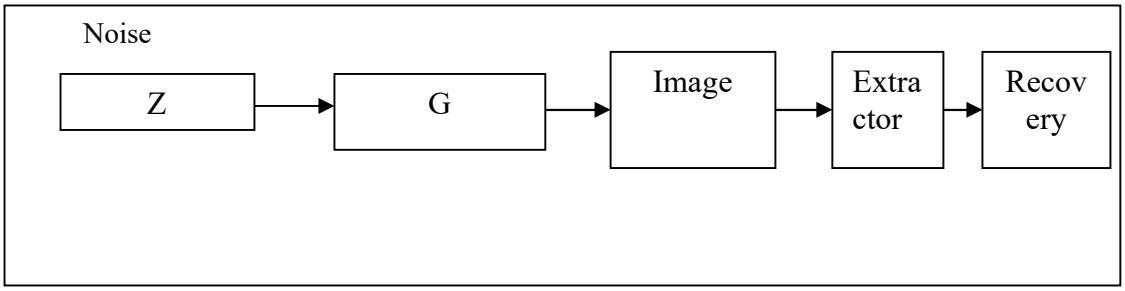



**Fig 7: Layers for CNN**

The original stego image has 64643 dimensions, whereas the output secret information noise vector has a size of 1100. Figure 8 depicts the extractor's training procedure.




**Algorithm II:** Extractor
Input : Stego Image
Output: Secret Information (D)
n=length (stego image)
for j=1 to n
$Y_i$= E (Stego image)
a=0
for i=1 to t do
$a=(V_{ij}+1) \times 2^{\sigma-1}j$
end for
Insert Di into D
end for

**Case III:** Secret Information Communication

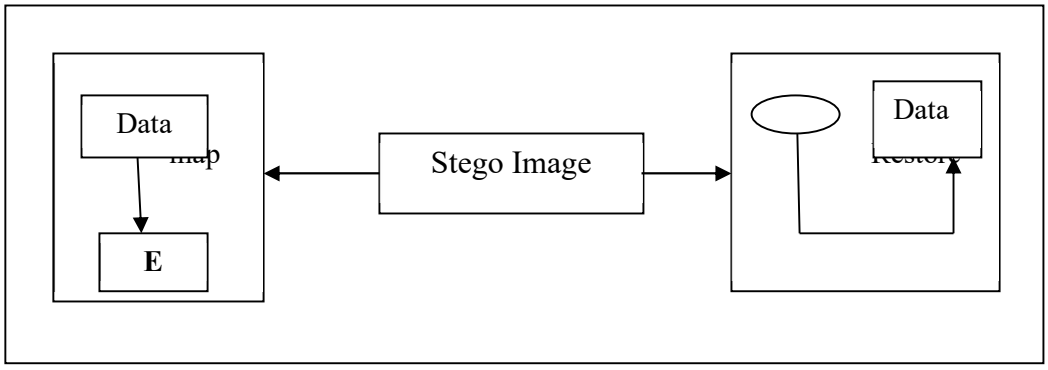



**Fig 9: Process for secret communication**

The data is sent to the CNN model, and the receiver receives the network parameters as well as the secret data. The transmitter calculates the noise vector by dividing the original data into pieces. The receiver receives the stego image and uses the mapping rules to recover the noise information and restore the secret information. The given data is in the form of image then the process is shown in Figure 10.

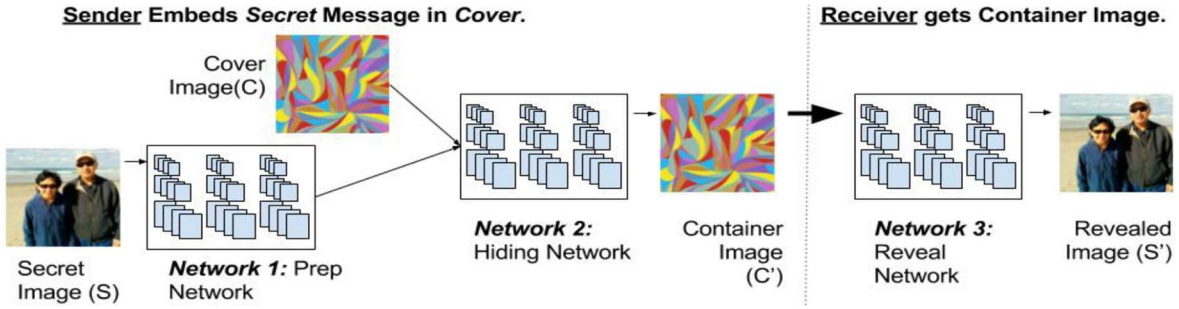



**Fig 10: Process for inserting image into an image**

There are three primary components in this technique. The secret image to be hidden is prepared using the Prep network. It will automatically alter the dimensions based on the secret picture and cover image sizes. In the first scenario, if the secret picture is smaller than the original image, the network size will be equal to the secret image's size. The hiding network combines the data from the cover picture and the prep network into a single container image. The cover picture and the hidden image are both present in this container network. It signifies that the scert image will be hidden in the cover image on this network. The reveal network takes the input from the container image and obtained the revealed imaged in the receiver side.

## IV. RESULTS AND ANALYSIS:

In this evaluation, we consider three different levels patch level, pixel level, and frame level. In frame level, each and every frame is taken into consideration for detecting anomalies. If at least one pixel in the frame is anomaly, it will identify as a anomalies frame. Pixel Level: In this level, the results are compared with the pixel of each frame. If more than 50% of the anomalies pixels are identified, then

the frame is to be considered as anomalies. Patch Level: In patch level, we focus on true and false measurements. When more anomalies are identified that one is treated as a true positive otherwise treated it as false positive. The Receiver operating characteristic curve (ROC) is used to measure the accuracy of the detected anomalies. The ROC curve consists of MPR and SPR

$$\text{MPR} = \frac{\text{True Positive}}{\text{True Positive+Fa Negative}} \quad (15)$$

$$\text{SPR} = \frac{\text{False Positive}}{\text{True Negative+False Positive}} \quad (16)$$

The performance is measured with Area under Curve, Equal Error Rate (EER) and Equal Detected Rate using the following formulas.

$$\text{EER=1-MPR for Frame Level} \quad (17)$$

$$\text{EDR=1-EER for Pixel level} \quad (18)$$

**Table 1: Comparison EER and AUC values of proposed algorithm with Existing algorithms**

| Algorithm | EER | AUC |
|---|---|---|
| SIF | 41% | 68.96% |
| MPS | 39% | 76.85% |
| MST | 26% | 83.45% |
| SRCS | 19% | 86.78% |
| Proposed | 12.34% | 91.6% |

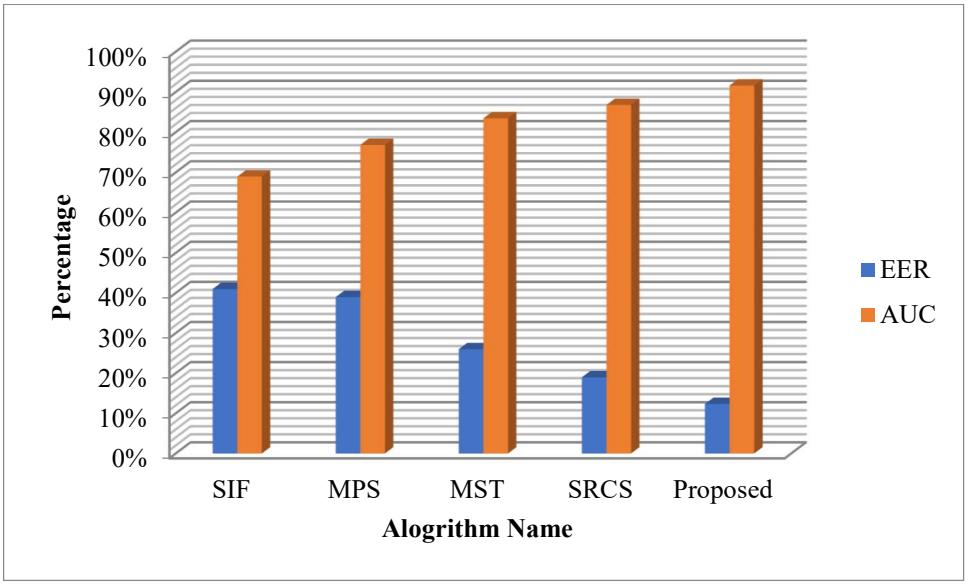



**Fig 11: Analysis of EER and AUC values of the proposed algorithm with Existing algorithms**

**Table 2: Comparison EDC and AUC values of the Proposed algorithm with Existing algorithms**

| Algorithm | EDC | AUC |
|---|---|---|
| SIF | 22% | 18.7% |
| MPS | 19% | 20.67% |
| MST | 47% | 43.23% |
| SRCS | 43% | 46.56% |
| Proposed | 58.49% | 68.74% |

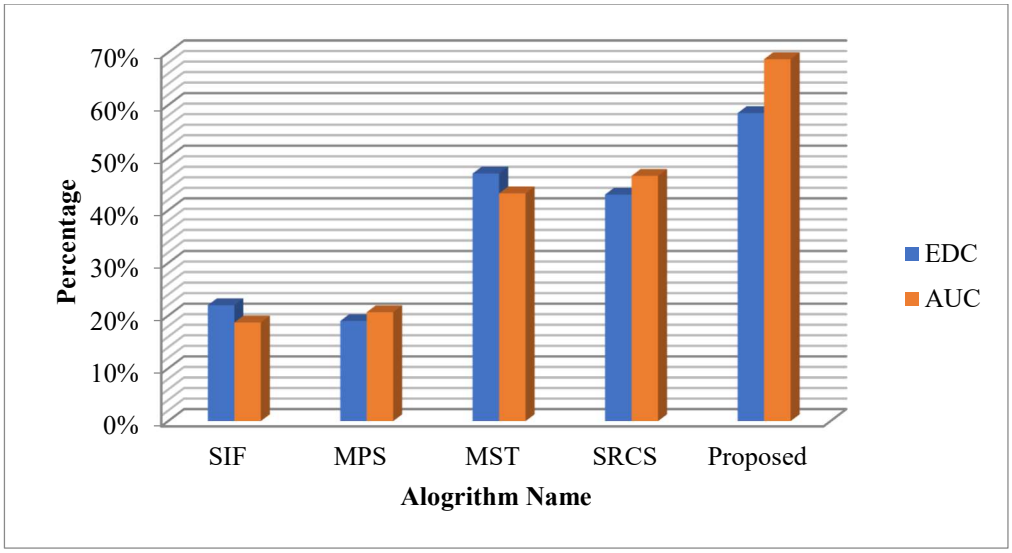



**Fig 12: Analysis of EDC and AUC values of the proposed algorithm with Existing algorithms**

**Table 3: Comparison EER and AUC values of proposed algorithm with Existing algorithms**

| Algorithm | EER | AUC |
|---|---|---|
| SIF | 41% | 68.96% |
| MPS | 39% | 76.85% |
| MST | 26% | 83.45% |
| SRCS | 19% | 86.78% |
| Proposed | 12.34% | 91.6% |

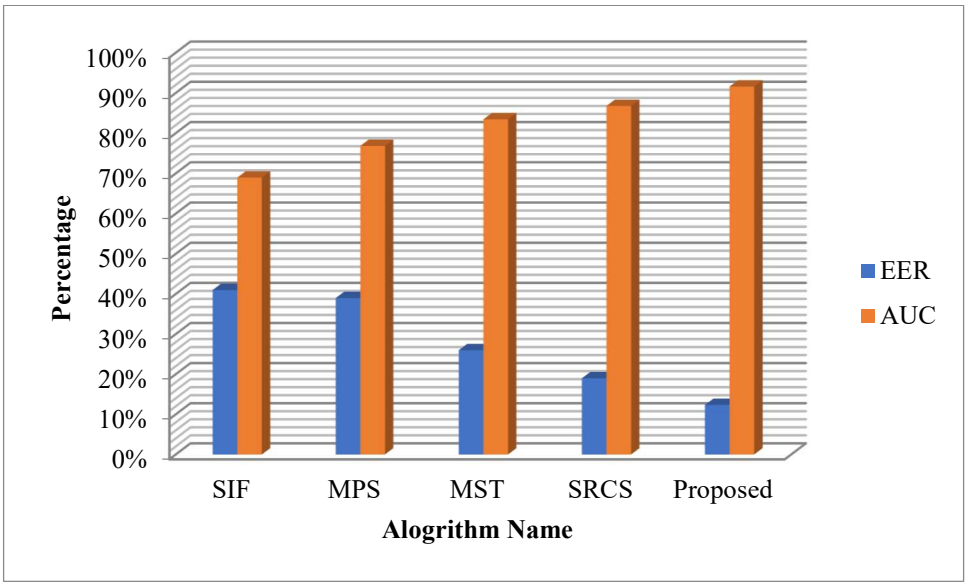



**Fig 13: Analysis of EER and AUC values of the proposed algorithm with Existing algorithms**

**Table 4: Comparison EDC and AUC values of the Proposed algorithm with Existing algorithms**

| Algorithm | EDC | AUC |
|---|---|---|
| SIF | 22% | 18.7% |
| MPS | 19% | 20.67% |
| MST | 47% | 43.23% |
| SRCS | 43% | 46.56% |
| Proposed | 58.49% | 68.74% |

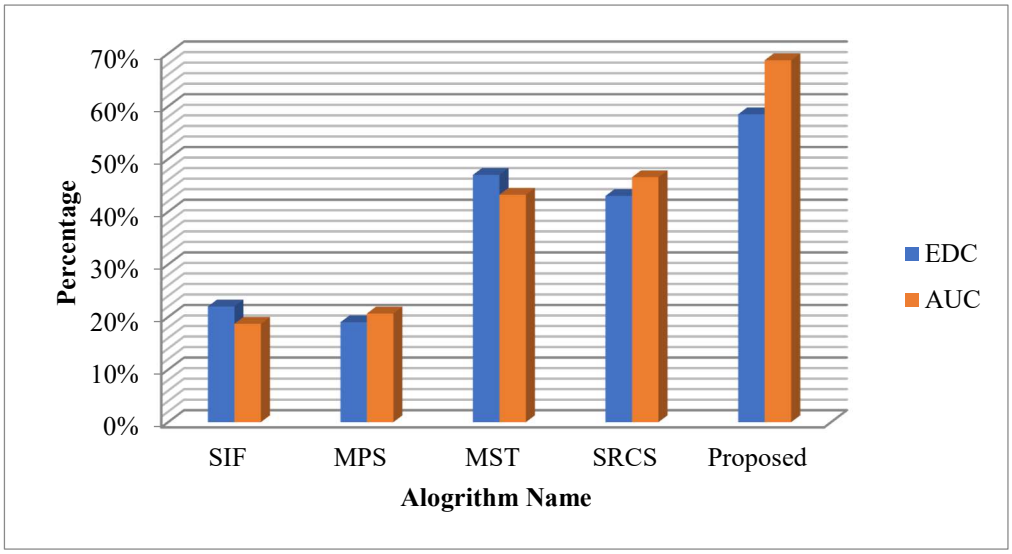



**Fig 15: Analysis of EDC and AUC values of the proposed algorithm with Existing algorithms**

The proposed model trained on two different data sets. Dataset 1 Celebrities, which contain 300 k different, face images of the humans and Food010, which contains 75 k food images. All those two datasets are cropped into 64 × 64 size.

Case I: Insert Image into cover Image

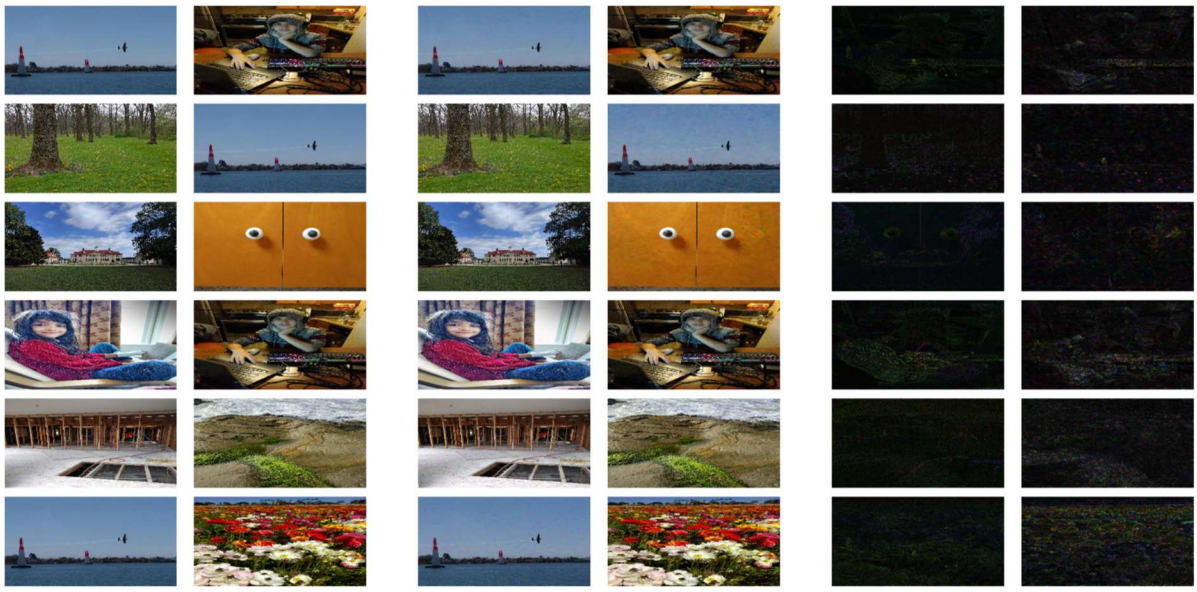


**Figure 16: Hiding Results ( Original image, secret image, cover image, embedding data with secret image, errors in between cover and hidden images)**

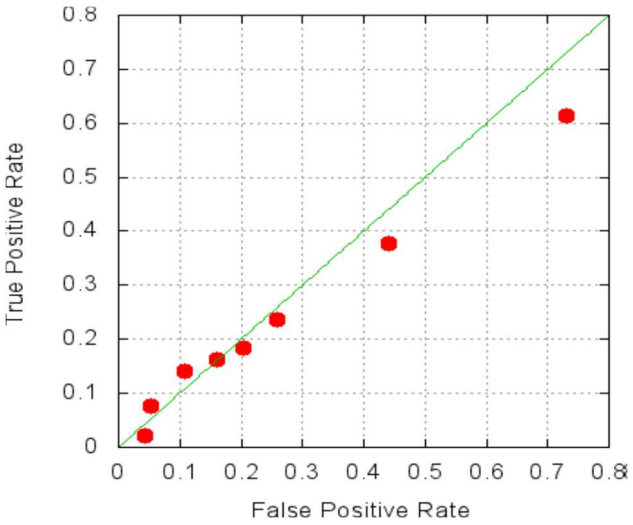



**Figure 17 : ROC Curve between True and False Positive rate**

**Case II:** Insert Textual data into cover image

In this experiment we trained with two different data set. The stego image is automatically generated by using training method and the data extracted using Conventional neural networks. The Table 5 shows absolute and relative capacities of various SWE existing method with proposed method


**Figure 18: Cover image after Phase I**

**Table 5: Comparison of Capacities of various SWE methods with Proposed Method**

| Algorithms | Capacity(Absolute) | Image Size | Capacity(Relative) |
|---|---|---|---|
| ZZHOU[18] | 1.215 | 512 ×512 | 4.88 ~3 |
| ZLHOUS[19] | 2.89 | 480 × 480 | 1.32~5 |
| S.AHANG[20] | 3.72 | 480 ×640 | 7.48-6 |
| J.XU[21] | 21~98 | 1024 ×512 | 8.45 -5 |
| WANG[22] | 64×32 | 1024 ×1024 | 6.40~3 |
| Proposed Method | >32.5 | 64 ×64 | 9.26 - 4 |

## V. CONCLUSION AND FUTURE SCOPE:

In this study firstly present novel approach for anomaly detection of crowd video using Deep Belief Networks (DBN). In this low-level features are extracted from spatiotemporal measurement, middle level features are extracted using three conventional mapping machines and high-level features are extracted from the fusion model. Match Subspace system and one class Support Vector Machines are used to detect anomalies from crowded videos and 3D image. Secondly a new approach in image steganography without embedding methods based on the automatic generation of the cover image. It means this approach generates stego images without embedding information into it. This algorithm is also suitable for hiding image into another stego image with the help of prep network, container and relief networks. The capacity of the proposed approach is tested with various existing algorithm of SWE method on various lengths of image sizes. If the size of image is high the capacity of the image

is little bit adequate. If the image size is low it produce better ratio with respect to relative and absolute capacities. The problem with larger image sizes can be resolved by incorporating error codes into this proposed method. These problems will be left as a future work. In Future more concentration has to be made to construct other than deep neural network architecture and different multi modal, fusion techniques for anomaly identification and detection for more complex videos.

**REFERENCES:**

[1] V. Mahadevan "Detection of anomalies in crowded scenes for 3D Images," in International Conference on Security and image processing), pp. 1985–1991, June 2016.

[2] A. A. Sodeemann, M. P. and B. J. Borgghetti, "A review of various anomaly detection in automated surveillance," security and its applications , , vol. 42, no. 6, pp. 1267–1272, 2016.

[3] M. Sabokrrou, , "anomaly detection and localization in crowded scenes for 2D and 3D images," in Proceedings of the IEEE Conference on multimedia and computer fusion pp. 2015.

[4] A. Deel Giorno, J., "A discriminative framework for anomaly detection in large videos for identifications," in Proceedings of the Italian Conferencce onComputer systems (ICSV'16), vol., 2016.

[5] B. Zhaoo, L. Feii-Feii, , " detection of various unusual events in videos via dynamic sparse coding and conventional coding," in Interantional Conference on Computer Security

[6] Moore, and M. Shah, "Chaootic invariants trajectories for anomaly detection in crowdedscenes," in Proceedings of the on Computer Security and Image Processing , pp. 2064–2070, San Francisco, Calif, USA, June 2017.

[7] A. Krizheevsky, I., "ImageNetclassification with deep convolutional neural networks," Communicationsof the ACM, and FEE vol. 60, no. 6, pp. 87–93, 2018.

[8] R. Giirshick, J., "Rich feaaturehierarchies for accurate object detection , object identification and semanticsegmentation," in 11th International conference on image processing

[9] C. Feichhtenhofer, A. Pinz, and A "Convolutional of two-stream network fusion for video action recognition and pattern ," inProceedings of the Interantional Confercne Communciations ), pp. 1933–1941,USA, July 2017

[10] N. Wanng and D.-Y. Yeuung, "Learning and testing deep compact imagerepresentation for visual tracking," in Advances in Networks and its applciations, pp. 819–827, 2016.

[11] J. Zhaung, "Autoencoder and decoder Networks (CFAN) for real-time face alignment and processing ," inProceedings of the Itlaian conference on computer security 2016.

[12] D. Xuy, Y. Yaan, J. Siong, and N. Seble, " Trining deep representationsof appearance and motion for anomalous event detection,"in Proceedings of the Confernce on vision (BMVC'16), Swansea, UK, 2016.

[13] Dr.D.Rathna Kishore, Dr.D.Suneetha A Secure Steganography Approach For Cloud Data Using Ann Along With Private Key Embedding", International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 6, June2018

[14] Y. Feng, Y Cahm, "Learning deep event models," Neurocomputing, vol. 219, pp. 558–566, 2017.

[15] T K. Jiayani , Y. Malise, "PCANet:a simple deep learning baseline for image classification and clustering ?" International Confernce on Image Processing, vol. 24, no. 12, pp. 5045-5056 2017.

[16] Wu. Li, V. Mahadeevan, and N. Vascoelos, “Anomaly detection and decentraliazaiiton localization in crowded scenes,” National Confernce on Pattern regocginition in new trends , vol. 36, no. 1, pp. 18–22, 2014.
[17] J.Kimannd Man“: a spacetimeMRF for detecting abnormal activities with incremental and external updates,” in Interantional conference recent ternds, pp. 2921–2928, June 2018.
[18] Dr.D.Rathna Kishore, Dr.D.Suneetha Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277- 3878, Volume-8 Issue-2, July 2019
[19] V. Reddy, “Improved anomalydetection in crowded scenes via cell-based analysis of foreground and background pixel speed, size and texture,” in Proceedings of the ComputerSociety Conference on Recent ternds in Computer), pp. 65–71, IEEE, June 2014.
[20] H. Leeko, R. Grosse rosma , “Learning componemts from supervised learning ,” Communications of the international conference on image processing and machine learning, vol. 54,
[21] Dr.D.Rathna Kishore, Dr.D.Suneetha “Deep Convolutional Neural Network based Image Steganogrpahy Technique for Audio- Image Hiding Algorithm” International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 –8958, Volume-9 Issue-4, April 2020
[22] Raja Bala Video Anomaly Detection 14 March 2018 Proceedings of the ComputerSociety Conference on Recent ternds in Computer), pp. 65–71
[23] Jones, M.J.; Ramachandra, A New Dataset And Evaluation Protocol For Video Anomaly Detection MITSUBISHI ELECTRIC RESEARCH LABORATORIES January 19, 2019
[24] Yingying Zhu” Context-Aware Activity Recognition And Anomaly Detection In Video” Ieee Journal Of Selected Topics In Signal Processing, Vol. 7, No. 1, January 2019