SECURE SURVEILLANCE FRAMEWORK USING PROBABILISTIC IMAGE ENCRYPTION

R. Dillibabu[#1], B. Lakshmibathy[#2], K. Mariya Dilip[#3], Mrs. J.Priskilla Angel Rani[*4]

[#1], [#2], [#3] *B.E, IV year, Department of Computer Science and Engineering*
[*4] *Assistant Professor, Department of Computer Science and Engineering*
Anand Institute of Higher Technology, Chennai

ABSTRACT

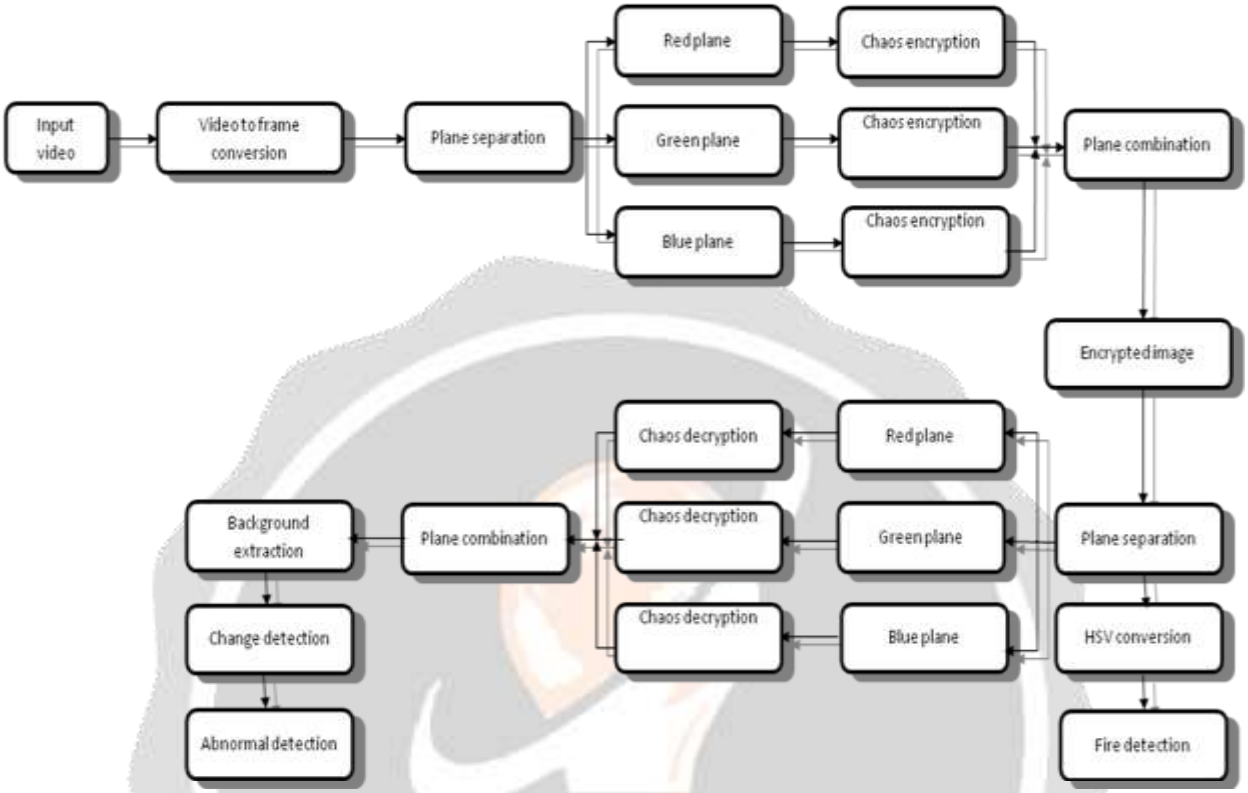
This paper proposes a secure surveillance framework for Internet of things (IoT) systems by intelligent integration of video summarization and image encryption. First, an efficient video summarization method is used to extract the informative frames using the processing capabilities of visual sensors. When an event is detected from key frames, an alert is sent to the concerned authority autonomously. As the final decision about an event mainly depends on the extracted keyframes, their modification during transmission by attackers can result in severe losses. To tackle this issue, we propose a fast probabilistic and lightweight algorithm for the encryption of keyframes prior to transmission, considering the memory and processing requirements of constrained devices that increase its suitability for IoT systems. Our experimental results verify the effectiveness of the proposed method in terms of robustness, execution time, and security compared to other image encryption algorithms. Furthermore, our framework can reduce the bandwidth, storage, transmission cost, and the time required for analysts to browse large volumes of surveillance data and make decisions about abnormal events, such as suspicious activity detection and fire detection in surveillance applications.

Keywords: *autonomously, probabilistic, abnormal, robustness, bandwidth.*

1. INTRODUCTION

The identification of objects in an image would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures.
The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skillful programming and lots of processing power to approach human performance. Manipulating data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer.
To digitally process an image, it is first necessary to reduce the image to a series of numbers that can be manipulated by the computer. Each number representing the brightness value of the image at a particular location is called a picture element, or pixel. A typical digitized image may have 512 × 512 or roughly 250,000 pixels, although much larger images are becoming common. Once the image has been digitized, there are three basic operations that can be performed on it in the computer. For a point operation, a pixel value in the output image depends on a single pixel value in the input image. For local operations, several neighbouring pixels in the input image determine the value of an output image pixel. In a global operation, all of the input image pixels contribute to an output image pixel value.

2.ARCHITECTURE DIAGRAM



3.ALGORITHM AND TECHNIQUES

3.1 Back ground Subtraction Algorithm

In basic method for Background subtraction, the static background image without object is taken first as a reference image. After that the current image of the video is subtracted pixel by pixel from the background image and resultant image is converted into binary image using threshold value. This binary image is worked as a foreground mask. For conversion in binary image threshold is required.
Illustration not visible in this excert,Where, the pixel intensity of frame at time t, B(x,y) is mean intensity on background pixel and T is threshold. When difference reaches beyond threshold the pixel categorize as a foreground pixel.

So the effectiveness of the object detection is depends on the threshold value.
Although this method is very fast, it is very sensitive to illumination changes and noise.
Illustration not visible in this except
1 Block Diagram of Simple Background Subtraction Method
2 Original Video Sequence
3 Simple Background Subtraction with Threshold 10
4 Simple Background Subtraction with Threshold 20
5 Block Diagram Of Mean Filtering Algorithm
6 Study Of Different Background Subtraction Algorithms

1.2 Neural Networks (CNN) :

We take an image, pass it through a series of convolutional, nonlinear, pooling (down-sampling), and fully connected layers, and get an output. That output can be a single class or a probability of classes that best describes the image.

CNN for digital image classification

The process of learning the parameters is called back propagation.
Feed an image to the network, and compare the output of the desired class, and pay a Loss in case of error.
Update the parameters by minimizing the Loss. Requires access the gradient of the loss as function of the parameters.

Data hiding method using IWT and BPCS, in which image data are decomposed by IWT and each bit plane of the sub-bands segmented in 8x8 blocks. All blocks are analyzed by complexity measures to determine which blocks will be replaced by secret message. The complexity measurement used in the proposed system is same one in the BPCS method. The proposed system can be recovered the hidden message in lossless manner if the communication channel is ideal. A wavelet transform that maps integers to integers is the transform**.**In this large amounts of data can be compressed as smaller one by using IWT method, without data loss. This system is used to produce same quality of image while compressing and embedding the image, there will be no change in the quality of image and can be retained the same as the first. By using BPCS (Bit Plane Complexity Segmentation) the embedding process has been done here, so the security is very high for the embedded image.

One example of wavelet transforms that mapintegers to integers is the *S-transform*. Its smooth(*s*) and detail (*d*) outputs for an index *n* are givenin (1a) and (1b) respectively (the smooth and thedetail outputs are the results of the application ofthe high-pass and the low-pass filtersrespectively).

The *S-transform* is reversible and its inverse is given in equations (2a) and (2b).

S (n) = [X(2n) + X(2n+1)]/2 … (1a)

d (n) = X(2n) - X(2n+1) … (1b)

X (2n) = s(n) + [(d(n) + 1)/2] … (2a)

X (2n + 1) = s(n) - d(n)/2 … (2b)

However, these equations should be in 2D inorder to be applied on images. In this section, wewill define the construction of the *2D Stransform*.

Suppose that the original image *(I)* is *Y* pixels wide and *X* pixels high. Denote the colour shade level of pixels located at position *i*and *j* by *Ii,j*. Generally, the 2D *S-transform* can becomputed for an image using equations (3a), (3b),(3c), and (3d). Of course the transform isreversible, i.e., we can exactly recover theoriginal image pixels from the computedtransform coefficients. The inverse is given inequations (4a), (4b), (4c), and (4d). The transform results in four classes of coefficients: (A) the low pass coefficients,(H) coefficients represent horizontal features of the image, (V) and (D) reflect vertical and diagonal information respectively. During the transform we ignore any odd pixels on the borders.

$$A_{i,j} = (I_{2i,2j} + I_{2i+1,2j}) / 2 \quad \text{(3a)} \qquad I_{2i,2j} = A_{i,j} - [H_{i,j} / 2] \quad \text{(4a)}$$

$$H_{i,j} = I_{2i,2j+1} - I_{2i,2j} \quad \text{(3b)} \qquad I_{2i,2j+1} = A_{i,j} + [H_{i,j} + 1) / 2] \quad \text{(4b)}$$

$$V_{i,j} = I_{2i+1,2j} - I_{2i,2j} \quad \text{(3c)} \qquad I_{2i+1,2j} = I_{2i,2j+1} + V_{i,j} - H_{i,j} \quad \text{(4c)}$$

$$D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j} \quad \text{(3d)} \qquad I_{2i+1,2j+1} = I_{2i+1,2j} + D_{i,j} - V_{i,j} \quad \text{(4d)}$$

Where, $1 \leq i \leq X/2$, $1 \leq j \leq Y/2$

Fig: (a) Input Image (b) Encrypted Image

3.3 Reversible Data Hiding VIA Optimal Code for Image

Data hiding in image processing may occur the permanent distortion and hence the original cover medium may not be able to be reversed exactly, after the hidden data have been extracted out. In our previous work, generalize the method of decompression algorithm as the coding scheme for embedding data and prove the codes can reach the rate–distortion bound as long as the compression algorithm reaches entropy and uses a binary covers for embedding messages. A code construction for recursive reversible data-hiding established a rate–distortion model. In our work presents a novel lossless data-embedding technique, which enables the exact recovery of the original image upon the extraction of the embedded information. After the Decompression, the original message will retrieve. The marked cover is reconstructed and extracting the original message from the cover.

A Reversible Data Hiding Method for Encrypted Images

The protection of this multi-media data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example.

Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step.

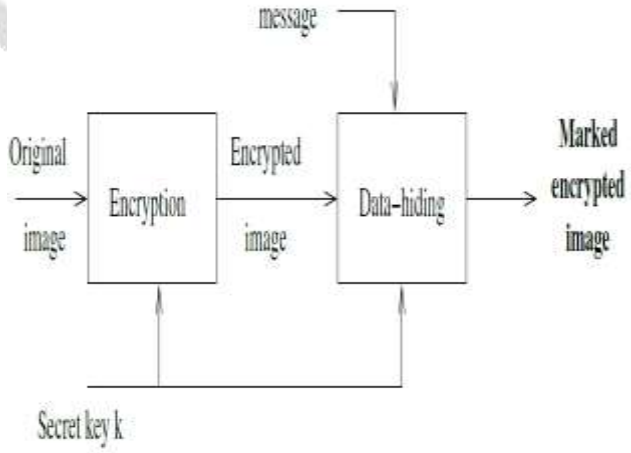


Fig: Embedding Process: Encrypted Image

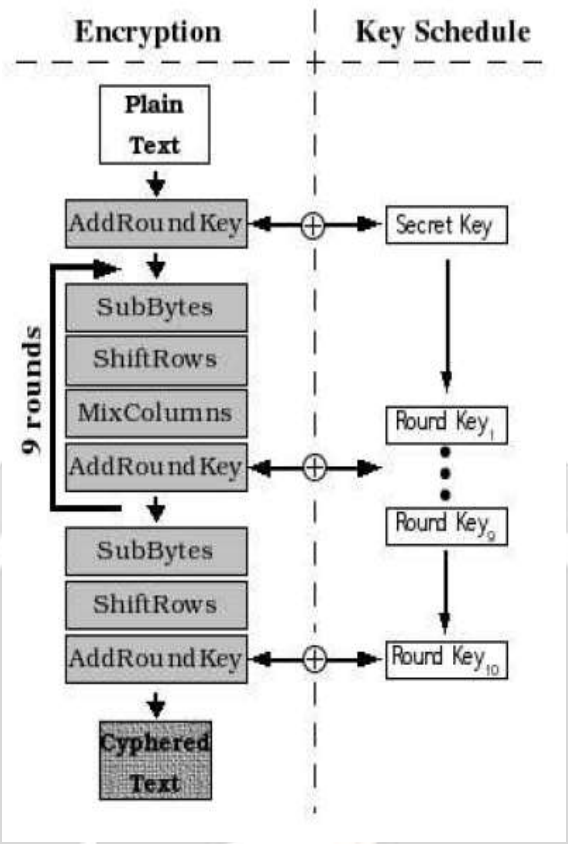


Fig: Encrypted Algorithm Process on Image: Algorithm Flow Chart

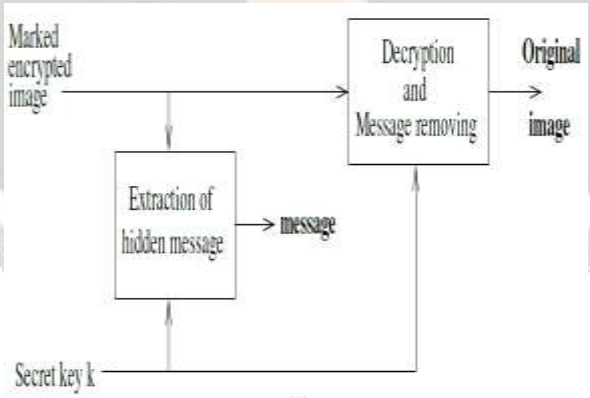


Fig: Extracting Process: Encrypted Image

Fig: (a) Input Image (b) Encrypt Image (C) Decrypt Image

REVERSIBLE data hiding (RDH) in images is a technique, by which the original cover can be loss lessly recovered after the embedded message is extracted. This important technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed.Since first introduced, RDH has attracted considerable research interest.

3D Image embedding Methods

Four steganography methods will be explored:

- Least Significant Bit Insertion
- Algorithms and Transformations
- Redundant Pattern Encoding
- Spread Spectrum Method

4.IMPLEMENTATION :

4.1 CAMERA :

In this module the camera is used to detect the activities that are happened in surroundings.
These gets input data in form of video.

4.2PLANE SEPARATION :

This module is used for conversion of frames by applying filters to the raw input that are obtained through camera. These conversions are gray scale, bilateral, red, green and blue separation.

4.2.1 CLASSIFICATION OF IMAGES:

There are 3 types of images used in Digital Image Processing. They are

- Binary Image
- Gray Scale Image
- Color Image

4.2.1.1 BINARY IMAGE:

A binary image is a digital image that has only two possible values for each pixel. Typically the two colors used for a binary image are black and white though any two colors can be used. Binary images are also called bi-level or two-level. This means that each pixel is stored as a single bit (0 or 1)

.

4.2.1.2 GRAY SCALE IMAGE:

A grayscale Image is digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray (0-255), varying from black (0) at the weakest intensity to white (255) at the strongest.
Grayscale images are distinct from one-bit black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white (also called bi-level or binary images).

4.2.1.3 COLOUR IMAGE:

A (digital) color image is a digital image that includes color information for each pixel. Each pixel has a particular value which determines it's appearing color. This value is qualified by three numbers giving the decomposition of the color in the three primary colors Red, Green and Blue. Any color visible to human eye can be represented this way. The decomposition of a color in the three primary colors is quantified by a number between 0 and 255. For example, white will be coded as R = 255, G = 255, B = 255; black will be known as (R,G,B) = (0,0,0); and say, bright pink will be : (255,0,255).

The four steps in a background subtraction algorithm are:

1. Pre-processing
2. Background modelling
3. Foreground detection
4. Data validation

4.2.2.1 Pre-processing:

This step consist of a collection of simple image processing tasks that change the raw input video into a format that can be processed by the next steps. In the early stage of processing, simple temporal or spatial smoothing are used to reduce noise such as rain and snow. In pre-processing, the data format used by the background subtraction algorithm is a very important key. Most of the algorithms handle luminance intensity, which is one scalar value per each pixel. However, color image, in either RGB or HSV colour space, is becoming more popular in the background subtraction literature [8, 15]. These papers argue that colour is better than luminance at identifying objects in low-contrast areas and suppressing shadow cast by moving objects. In addition to colour, pixel-based image features such as spatial and temporal derivatives are sometimes used to incorporate edges and motion information. For example, intensity values and spatial derivatives can be combined to form a single state space for background tracking with the Kalman filter. Plessy et al. combine both spatial and temporal derivatives to form a constant velocity background model for detecting speeding vehicles. The main drawback of adding colour or derived features in background modelling is the extra 130 Computer Science & Information Technology (CS & IT) complexity for model parameter estimation. The increase in complexity is often significant as most background modelling techniques maintain an independent model for each pixel.

4.2.2.2 Background Modelling:
Background modelling is at the heart of any background subtraction algorithm. Much research has been devoted to developing a background model that is robust against environmental changes in the background, but sensitive enough to identify all moving objects of interest. We classify background modelling techniques into two broad categories, no recursive and recursive. They are described in the following subsections. • Non-recursive techniques: A non-recursive technique uses a sliding-window approach for background estimation. It stores a buffer of the previous L video frames, and estimates the background image based on the temporal variation of each pixel within the buffer [6]. • Recursive Techniques: Recursive techniques do not maintain a buffer for background estimation. Instead, they recursively update a single background model based on each input frame. As a result, input frames from distant past could have an effect on the current background model [6]. Recursive techniques require less storage not like no recursive techniques, but any mistake or error in the background model can lead us to a much longer period of time.

4.2.2.3 Foreground detection:

This step makes us able to compare the input video frame with the background model, and identifies foreground pixels from the input frame. There is some techniques that doesn't use the same image as a background model like the Mixture of Gaussian model (MoG), but the most of techniques use a single image as their background models, so the approach for foreground detection is to check whether the input pixel is different from the corresponding background estimate [17]: $|It(x,y) – Bt(x,y)| > T$ (6) Another popular foreground detection scheme is to threshold based on the normalized statistics: $(|It(x,y) – Bt(x,y) - \mu d| / \partial d) > Ts$ (7) Where μd and ∂d are the mean and the standard deviation of $It(x, y) – Bt(x, y)$ for all special locations (x; y). Most schemes determine the foreground threshold T or Ts experimentally [17].

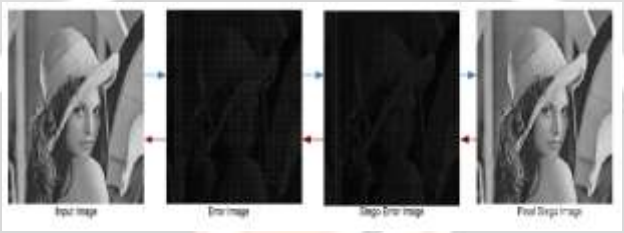
1.2.2.4 Data Validation:

To improve the candidate foreground mask based on information obtained from outside the background model, we define data validation process. All the background models have three main limitations: First, they ignore any correlation between neighboring pixels; second, the rate of adaptation may not match the moving speed of the foreground objects; and third, non-stationary pixels from moving leaves or shadow cast by moving objects are easily mistaken as true foreground objects. When the background model adapts at a slower rate than the foreground scene, large areas of false foreground, commonly known as ghosts, often occur. Sophisticated vision techniques can also be used to validate foreground detection. Computing optical flow for candidate foreground regions can eliminate ghost

objects as they have no motion. Colour segmentation can be used to grow foreground regions by assuming similar colour composition throughout the entire object.

4.2.3 Prediction-based Reversible Data Hiding Using Empirical Histograms in Images:-

A multilevel reversible data hiding method based on histogram shifting which can recover the original image loss lessly after the hidden data has been extracted from the stego-image. The method of prediction is adopted in our proposed scheme and prediction errors are produced to explore the similarity of neighbouring pixels. In this article, we propose two different predictors to generate the prediction errors, where the prediction is carried out using the centre prediction method and the JPEG-LS median edge predictor (MED) to exploit the correlation among the neighbouring pixels. Instead of the original image, these prediction errors are used to hide the secret information. Moreover, we also present an improved method to search for peak and zero pairs and also talk about the analogy of the same to improve the histogram shifting method for huge embedding capacity and high peak signal-to-noise ratio (PSNR). In the one-level hiding, our method keeps image qualities larger than 53 dB and the ratio of embedding capacity has 0.43 bpp (bit per pixel). Besides, the concept with multiple layer embedding procedure is applied for obtaining high capacity, and the performance is demonstrated in the experimental results.



5.APPLICATIONS

- Public area
- Remote area

6.EXISTING SYSTEM

- Motion detection cameras will capture the environment when the motion is occurred.
- There is no surveillance camera to find the abnormality in the localized area.

7.CONCLUSION

This System is used to find the abnormal activity and also used to find the fire detection without need of human . This system also captures image and its sends to particular authority that time itself.

REFERENCE

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, pp. 2233-2243, 2014.
[2] M. Sajjad, I. Mehmood, and S. W. Baik, "Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network," *Sensors*, vol. 14, pp. 3652-3674, 2014.
[3] J. Lloret, I. Bosch, S. Sendra, and A. Serrano, "A wireless sensor network for vineyard monitoring that uses image processing," *Sensors*, vol. 11, pp. 6165-6196, 2011.
[4] I. Mehmood, M. Sajjad, W. Ejaz, and S. W. Baik, "Saliency-directed prioritization of visual data in wireless surveillance networks," *Information Fusion*, vol. 24, pp. 16-30, 2015.

[5] R. Hamza, K. Muhammad, Z. Lv, and F. Titouna, "Secure video summarization framework for personalized wireless capsule endoscopy," *Pervasive and Mobile Computing*, 2017..
[6] D. Zhang, G. Li, K. Zheng, X. Ming, and Z.-H. Pan, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE transactions on industrial informatics*, vol. 10, pp. 766-773, 2014.
[7] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Information Security Journal: A Global Perspective*, vol. 25, pp. 162-179, 2016/12/01 2016.