

Comparative Analysis of Video Steganography Techniques

T. Muthu Lakshmi, P. Mohamed Fathimal, P. Arockia Jansi Rani

Department of Computer Science and Engineering, Manomaniam Sundaranar University, Tirunelveli, India

Department of Computer Science and Engineering, Manomaniam Sundaranar University, Tirunelveli, India

Department of Computer Science and Engineering, Manomaniam Sundaranar University, Tirunelveli, India

ABSTRACT: In the intricately connected world of E-commerce, secure data transmission is of prime importance. To keep the hackers unaware of secret data transmission, many techniques are used. Steganography is the process of embedding secret data into data sources such as audio, video, or image signals without changing perceptual quality. The most common techniques for embedding data is the use of least significant bit and the use of redundancy in the cover image by performing lossless compression. This paper discusses the three methods-- Least Significant Bit, Vector Quantization and Motion Vector method for embedding the secret image in a compressed video. This chapter analyses these three methods and to evaluate the performance of these methods, the various test images are used in the experiments. The results are compared in terms of visual quality of the recovered image, embedded video and compression ratio.

KEYWORDS: Data Hiding, Encryption, Compression, Video Steganography, Motion Vector Based Steganography.

I. INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It is the art of concealing a message in a cover without leaving a remarkable track on the original message. There are 4 different types of steganography -Text, Audio, Image and Video.

The rest of this paper is organized as follows-Section II discusses the related works. Section III discusses the Least Significant Bit, Vector Quantization and Motion Vector method for embedding the secret image in a compressed video. Section IV discusses the experimental result and finally section V concludes the paper.

II. RELATED WORK

D. Fang et al [1] proposed Data hiding for digital video with phase of Motion Vector (MV). In this paper, the authors proposed an effective data-hiding scheme that embeds data in digital videos using the phase angle of the motion vector of the macro block in the inter-frame the embedded data can be extracted directly without using the original video sequences.

H. Aly et al [2] proposed Data hiding in Motion Vectors of compressed video based on their associated prediction error. It deals with data hiding in compressed video. The Motion Vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bit stream is embedded in the least significant bit of both components of the candidate motion vectors. Y. Cao et al [3] proposed Video steganography with perturbed motion estimation. In this paper, the authors proposed the approach that targets the internal dynamics of video compression. Inspired by Fridrich et al's Perturbed Quantization (PQ) steganography, a technique called Perturbed Motion Estimation (PME) is introduced to perform motion estimation and message hiding in one step. Intending to minimize the embedding impacts, the perturbations are optimized with the hope that these perturbations will be confused with normal estimation deviations.

Cao et al [4] proposed Video steganalysis exploiting motion vector reversion-based features. In this paper, the mot MV

based methods target the internal dynamics of video compression and embed messages while performing motion estimation. The authors design a calibration-based approach and propose MV reversion-based features for steganalysis. Experimental results demonstrate that the proposed features are very sensitive to the tendency of MV reversion during calibration and can be used to effectively detect some typical MV-based steganography even with low embedding rates. Wang et al [5] proposed Video steganalysis against motion vector-based steganography by adding or subtracting one MV value. In this paper, the modification on the Least Significant Bit (LSB) of the Motion Vector is modeled. The influence of the embedding operation on the Sum of Absolute Difference (SAD) is illustrated, which allows us to focus on the difference between the actual SAD and the locally optimal SAD after the adding-or-subtracting-one operation on the motion value. Finally, because most Motion Vectors are locally optimal for most video codec's, two feature sets are extracted and used for classification.

C. C. Chen et al [6] have proposed High capacity Side Matching Vector Quantization (SMVQ) based hiding scheme using adaptive index. In this paper, a high-capacity image-hiding scheme based on an adaptive index was proposed. Data-hiding based on VQ is a technique for hiding data in the VQ index code. Data-hiding based on Side Match Vector Quantization has been proposed for improving the compression rate of VQ-based data-hiding schemes. However, the hiding capacity of an SMVQ-based data-hiding scheme is very low since, at most, only one secret bit is hidden in one index code. According to the experimental results, a higher hiding capacity was obtained and a good-quality embedded image was preserved in the adaptive index SMVQ-based data-hiding scheme. P. Tsai [7] proposed Histogram-based reversible data hiding for vector quantization compressed images. In this paper, Reversible data hiding is required and preferable in many applications such as medical diagnosis, military, law enforcement, fine art work and so on was proposed. The author proposed to use reversible data hiding applications with a vector quantization compressed image. The histogram of the prediction VQ-compressed image is explored. The prediction VQ encoded image is identical to traditional VQ encoding. The index of prediction encoded VQ images is modified to embed secret data. Furthermore, the VQ images can be completely reconstructed by the recovery procedure.

J. D. Lee et al [8] proposed reversible data hiding of SMVQ indices. In this paper, the author proposes reversible data hiding based on histogram modifications on SMVQ indices. Chang et al [9] developed another index-modifying data-hiding scheme with recovery capability. In this paper, Indicators are added in front of the most encoded indices and Only two clusters can be used to hide secret data in their 2-bit hiding scheme, resulting in low embedding capacity and high bit rate (BR). In general, high embedding capacity can be achieved with SMVQ-based data-hiding schemes, in which a state codebook is used to encode each index, yet they require more encoding time than that of the index-modifying techniques. Shie et al. [10] developed an adaptive data hiding based on a VQ-compressed image. In this paper, SMVQ modifying technique was proposed. The image blocks are classified into embeddable and unembeddable blocks based on the variances and side-match distortions (SMDs). Although this scheme can yield a high embedding capacity, the quality of the reconstructed image reduces as the quantity of secret data increases. In addition, this scheme is a case of the irreversible information hiding.

C. C. Chen et al [11] proposed High capacity SMVQ-based hiding Scheme using adaptive index. In this paper both VQ and SMVQ are used to hide secret data, in which a 1-b indicator is always required for each index and only 1-b secret data can be embedded in each index when the VQ technique is applied. Conversely, more than one bit secret data can be embedded in each index when the SMVQ technique is applied. This scheme can provide a higher hiding capacity, yet it is also an irreversible data-hiding scheme. RonakDoshi et al [12] proposed Steganography and its applications in security using LSB coding. The simplest approach to hiding data within the video file is called least significant bit (LSB) insertion was proposed. In this method, the authors take the binary representation of the hidden data and overwrite the LSB of each byte within the cover video. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye.

Mr. Vikas Tigay [13] proposed Data Hiding in Image using least significant bit with cryptography. To increase the security of messages sent over the internet steganography is used. This paper discussed a technique used on the LSB (least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

III. VIDEO STEGANOGRAPHY ALGORITHMS

This section discusses the procedure of three video steganography techniques- LSB based method, VQ based steganography, block based motion vector steganography for secure transmission of a secret image. These methods use the video as a cover media for hiding the secret information.

A. Procedure for embedding Secret Image in a video

For secure data transmission with high embedding capacity, the cover video is compressed and encrypted using scalable Encryption Algorithm. The compression technique removes the redundant data's from the video frames. Therefore, the large amount of data can be hidden in a video

Embed the secret image in a video using any one of the three steganography methods- LSB, VQ Based and Motion Vector based Method.

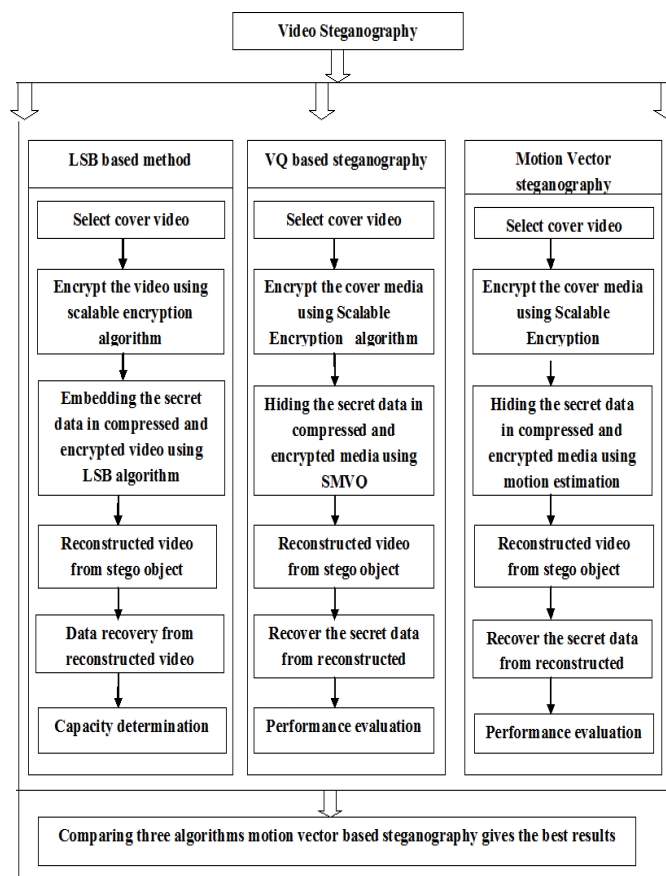


Figure 1 System Design

Fig 1 shows the System Design that describes about overall view for methodology of each steganography algorithm such as LSB based method, VQ based steganography, block based Motion Vector steganography and performance metrics are calculated to evaluate the above three algorithms. These methods use the video as a cover media for hiding the secret information. For achieving the secure data transmission and embedding the large amount of data it compress and encrypt the video using some compression methods. The compression technique removes the

redundant data's from the video frames. So the large amount of data will be hidden in a video. Then the secret data will be hidden in a compressed video using some algorithms. These compression methods and embedding algorithms are implemented. After implementation is done the secret message is extracted.

B. Scalable encryption:

The main goal of scalable encryption is to encrypt and to reduce the amount of data to be encrypted. After encryption, it performs compression on inter frames and remove the redundant pixel values on frames. Most of the conventional algorithms are not useful for image encryption because of the redundant data contained in an image, strong correlation between the pixel value of the image and high computational complexity of the algorithm. For this purpose, scalable encryption is used, which provide security and confidentiality for secure transmission of data through the network.

Algorithm for Scalable Encryption:

- 1: Input and colored video (which contains R (Red), G (Green), B (Blue) pattern).
- 2: Use the technique of confusion and diffusion to replace each pixel of the input video by another value generated by random number generator.
- 3: After generating the random numbers, that random numbers will be XOR ed with the original pixel to get an encrypted video.

C. LSB based method

Compression method for LSB algorithm

For compressing video the index-modifying technique can be applied to compress the indices. Compression accompanied by the index-modifying technique can yield a lower embedding capacity and a higher bit rate, yet less time consuming. The neighboring processed indices are employed to speed up the processes of generating state Codebooks required for encoding and hiding.

Vector quantization (VQ) has widely been used for signal processing due to its excellent compression performance. Data hiding techniques in the VQ-compressed domain can relish advantages of both data hiding and compression for a multimedia distribution, achieving a secure channel and bandwidth/space saving for data transmission/storage

Data embedding procedure:

This method is used to hide the data in compressed videos. Cover-video with the hidden messages added in them are called stego-object. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-video with the secret message bits. LSB methods typically achieve high capacity. This allows a person to embed the data in the cover video and make sure that no one could detect the secret information in the cover media. The LSB method does not increase the file size, but depending on the size of the data that is to be hidden inside the cover media, that can become distorted.

Algorithm steps for LSB method

1. Determine an encrypted video (cover video).
2. Determine the secret message or data that should be embedded into the cover media.
3. Convert all the pixel values of the encrypted video from grayscale to 8-bit binary values.
4. Embed the secret message or data into the cover media by hiding the data into the LSB bit of cover video.
5. The data from the cover media is recovered with less distortion and the PSNR value is calculated.

Data-extraction procedure

At the receiver, the decoder can recover the embedded secret information and reconstruct the original VQ indices simultaneously. Initially, the first $\log_2(cs)$ bits are read from the code stream bs. The first index that is the base index of the first row of the original VQ-compressed image is restored by the $\log_2(cs)$ bits. After restoring the base index, each index can be predicted by its corresponding prediction index. Let rx and rv represent the restored index and the value retrieved from the code stream with length $\log_2(cs)$ bits. For an unpredictable index, the restored index rx can be obtained by

$$rx = rv \quad (1)$$

The encoded index can be a predictable index or unpredictable index according to its corresponding prediction value. As mentioned above, an unpredictable index can be easily restored. For a predictable index, Jv bits converted to a decimal value Jv is read from the code stream bs, and then considered as an indicator. The encoded index can be identified as one of the following indices by the value of Jv .

D. Vector Quantization Based Method

Hiding the secret information into vector quantization (VQ)-compressed videos that can be lossless and the

compressed video is reconstructed after the secret data is extracted in the decoder. For VQ-compressed videos, the index-modifying and the side-match VQ (SMVQ) techniques can be applied to encode indices and to hide secret data. Data hiding accompanied by the SMVQ technique can yield a higher embedding capacity and a lower bit rate and more time consuming.

Data embedding method using BMC

1-b indicator is required for each index and only 1-b secret data can be embedded in each index when the VQ technique is applied. More than one bit secret data can be embedded in each index when the SMVQ technique is applied. The VQ consists of three phases. They are codebook generation, encoding process, and decoding process. A codebook is generated from a set of training images. With a generated codebook, each block in an image is encoded using the index of the nearest codeword of the block such that the total storage space for an image is significantly reduced. In the decoder process, with the same codebook as that used in the encoder, the original image is restored from the indices using a table-lookup operation.

Algorithm steps

Input: A grayscale image G of size $N * M$; a

Output: The code stream in a binary form bs with the parameters $J, I, V - th$, and s

Offline preprocessing:

1. Calculate the mean value, variance value, and p value for each codeword in the codebook.
2. Rearrange the codeword's of codebook in ascending order according to the mean values, variance values.

Online processing

1. Compress video G using VQ to obtain a VQ compressed image CI of size $(N/n) * (M/m)$ where $n * m$ denotes block size.
2. Read the next index and the p value of the prediction index, denoted as C and p , from the VQ-compressed image in the raster scan order.
3. If p is 0, $bs = bs || c$ then, where $||$ denotes the concatenation operation, then go to Step 7.
4. If C is a short index, then:
 - Calculate the $BMC - s$ of C ;
 - Take a, sd from the secret data stream
 - $bs = bs || BMC - s || sd$. Go to step 7
5. If C is a middle index, then:
 - Calculate the $BMC - m$ of C ;
 - $bs = bs || (2^J - 2) || BMC - m$. Go to Step 7.
6. If C is a long index, then $bs = bs || (2^J - 1) || C$.
7. Repeat Steps 2-7 until all of the indices in the VQ-compressed image are processed.
8. Output the code stream bs and parameters J, I, Vth and s .

Data-extraction steps

Input: The code stream in binary form bs with the parameters $J, I, V - th$, and s .

Output: The reconstructed VQ image G_* of size $N * M$ and retrieved secret data stream.

1) Offline preprocessing:

- Calculate the mean value, p value and variance value of each codeword in the codebook.
- Rearrange the codeword's in ascending order according to their means, variances, and Vth .
- Calculate the values of Ks and Km .

2) Online processing:

- Set $ptr = 1$; Set $restoredsd = Null$.
- If the prediction value = 0 (un prediction), then Read the next $log_2(cs)$ bits from the code stream bs , $resorted\ index = B2D(bs(ptr:ptr + log_2(cs)))$, where $B2D(x)$ denotes the binary to the decimal operation.
- If the prediction value = 1 (prediction), then read next J bits from the code stream bs , $indicator = B2D(bs(ptr:ptr + J - 1))$, $ptr = ptr + J$. If the value of the indicator lies in between 0 and $2^J - 3$, then $restored\ index = indicator + Ks$ $restored\ sd = read\ the\ next\ s\ bits\ from\ the\ code\ stream\ bs$, $restored\ sd = restored\ sd || restored\ sd$.
- If the indicator = $2^J - 2$, then read the next I bits from the code stream bs , $lv = B2D(bs(ptr:ptr + I -$

- 1)), $ptr = ptr + I$, restored index = $Iv + Km$.
- If the indicator = $2\lambda J - 1$, then read the next $\log_2(cs)$ bits from the code stream bs *resorted index* = $B2D(bs(ptr:ptr\log_2(cs) - 1))$, $ptr = ptr + \log_2(cs)$ Repeat Steps 2–4 until all of the bits in the code stream are processed.
- Output the reconstructed VQ image and restored the secret data.

F. Motion Vector based steganography

This method goal is to improve the security of motion vector-based steganography. This method suggests that the perfect security (undetected) can be approached if the uncertain information, which exists in the process of motion estimation, is fully exploited and establishes a connection between single motion vectors' embedding distortion and its associated uncertainty.

Data embedding

The sender has some raw video frames comprising of N blocks in all, and wants to communicate an αN -bit message m to the recipient. To begin with, these raw frames are fed into a customized encoder for compression. For $i = 1$ to N , the i th block is subjected to ME processes with different λ values, and its default MV mvi together with the associated uncertainty di are obtained and calculated. After that, a binary channel $P = (p_1, \dots, p_N)$ is formed by the parity check function

$$p(mv) = LSB(h + V) \quad (2)$$

Where LSB refers to the least significant bit of a binary integer, h and v denote the MV's horizontal and vertical components, and $pi = P(mvi)$. Meanwhile, the distortion scale vector $\Gamma = \gamma_1, \dots, \gamma_N$ is calculated. After the coding process, the raw frames are fed into the encoder again. For $i = 1$ to N , the i^{th} block is subjected to a perturbed ME process, if $pi = pi$, its MV mvi is left unchanged; otherwise, a full search procedure centering around mvi is conducted to find a new MV as

$$\overline{mvi} = \arg_{mv \in M(\overline{pi})} \min SAD_{mv} \quad (3)$$

Where $M(\overline{pi})$ is the set of all possible MVs satisfying $P(mv) = \overline{pi}$. Finally, the compressed frames are obtained with MVs carrying secret message bits.

K. Data extraction

Compared to the embedding process, the message extraction is much easier. With the received compressed frames, the recipient can use a common decoder to read the MV values, then recover the binary channel p , finally extract the secret message using

$$Ext\ stc(\hat{p}) = \hat{p}H = m \quad (4)$$

In this method, a novel MV-based steganography is proposed, which reduces the probability of detection significantly with respect to the current best steganalytic method.

IV. EXPERIMENTAL RESULTS

The video steganography schemes are implemented in Mat lab 10.0 running on Windows8. Experiments performed on i5 Processor with 4 GB of memory. To illustrate, input secret image of size 150*100 for embedding in a video file. The criteria for the visual quality of the image is the peak signal to noise ratio, which is defined as

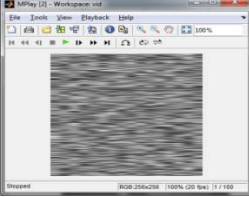

$$MSE = \frac{1}{mn} \sum_1^m \sum_1^n [I_{ij} - I'_{ij}]^2 \quad (1) \quad PSNR = 20 * \log_{10}(\max_f / \sqrt{MSE}) \quad (2)$$

I -original image of size $m \times n$

I' -recovered image of size $m \times n$ $[\max]_f$ - maximum intensity value that exists in the Original image (255).

The higher the PSNR value, better the quality of the reconstructed image. To test the visual quality of the image and to compare the performance of the three techniques, the test image Jet F16 with size 481*321 has been taken as the secret image while the cover (stego) video of size 1.36 MB. The average PSNR for the cover image is 54.96dB.

Table I Experimental Results of Three algorithms

Input	Video	Secret Image
Encrypted and Compressed video with secret message		
LSB based method	Video after extraction	Extracted Image
SMVQ based method	Video after extraction	Extracted Image
MV based steganography	Video after extraction	Extracted Image

This Table I show the experimental results of three algorithms LSB method, VQ based method and MV based steganography method

Table II Performance analysis of three algorithms

Video.avi	Image 1.tif			Image 2.png			Image 3.jpeg		
	LSB	VQ	MV	LSB	VQ	MV	LSB	VQ	MV
Performance Measures	LSB	VQ	MV	LSB	VQ	MV	LSB	VQ	MV
Compression Ratio	59.1016	59.1016	79.1016	59.1016	59.1016	79.1016	59.1016	59.1016	79.1016
PSNR(original and Compressed video)	22.9408	22.9408	22.9408	22.9408	22.9408	22.9408	22.9408	22.9408	22.9408
PSNR (original and Reconstructed Video)	33.7050	38.8525	48.8525	35.3421	38.8525	48.8525	38.8525	38.8525	48.8525
Peak-Signal-to-Noise Ratio (Image)	48.2348	44.3199	61.4798	44.4563	48.3270	53.9905	42.1880	45.9401	57.3718
Correlation	0.7769	0.8844	0.9945	0.7733	0.8756	0.9857	0.7673	0.7757	0.9885
Data Hiding Rate(in Bytes)	44746	101434	101434	82545	529943	529943	70468	54207	70468
Bit Error Rate	0.1311	0.0386	0.0185	0.1386	0.0691	0.0490	0.1657	0.1498	0.0456

Table II shows the performance analysis of three algorithms with different image formats.

V. CONCLUSION

In this paper, we compare the performance analysis of video seganographic algorithms. The MV based method has a low complexity and it is easy to implement. After applying the performance metrics in these three algorithms it is analyzed that MV based steganography given better results as compared with SMVQ technique and LSB Image hiding technique .So overall compression ratio of the image will be very high and the image resolution remains good for image hiding applications.

REFERENCES

- [1] D. Fang and L. Chang, "Data hiding for digital video with phase of motion vector," in Proc. IEEE Int. Symp. Circuits Syst., 2006, pp. 1422–1425.
- [2] H. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 14–18, Mar. 2011.
- [3] Y. Cao, X. Zhao, D. Feng, and R. Sheng, "Video steganography with perturbed motion estimation," in Proc. IH, vol. 6958, LNCS, 2011, pp. 193–207.
- [4] Y. Cao, X. Zhao, and D. Feng, "Video steganalysis exploiting motion vector reversion-based features," IEEE Signal Process. Lett., vol. 19, no. 1, pp. 35–38, Jan. 2012.
- [5] K. Wang, H. Zhao, and H. Wang, "Video steganalysis against motion vector-based steganography by adding or subtracting one motion vector value," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, pp. 741–751, May 2014.
- [6] C. C. Chen and C. C. Chang, "High capacity SMVQ-based hiding Scheme using adaptive index," Signal Process., vol. 90, no. 7, pp. 2141–2149, 2010.
- [7] P. Tsai, "Histogram-based reversible data hiding for vector quantization compressed Images," IET Image Process. vol. 3, no. 2, pp. 100–2114, 2009
- [8] J. D. Lee, Y. H. Chiou, and J. M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices," IEEE Trans. Informat. Forensics Security, vol. 5, no. 4, pp. 638–648, Dec. 2010.
- [9] C. C. Chen and C. C. Chang, "High capacity SMVQ-based hiding scheme using adaptive index," Signal Process., vol. 90, no. 7, pp. 2141–2149, 2010.]
- [10] S. C. Shie, S. D. Lin, and C. M. Fang, "Adaptive data hiding based on SMVQ prediction," IEICE Trans. Informat. Syst., vol. E89-D, no. 1, pp.358–362, 2006.

- [11] C. C. Chen and C. C. Chang, "High capacity SMVQ-based hiding Scheme using adaptive index," Signal Process. vol. 90, no. 7, pp. 2141–2149, 2010.
- [12] C. Zhu, X. Lin, and L. Chau, "Hexagon-based search pattern for fast block motion estimation," IEEE Trans. Circuits Syst. Video Technol., vol. 12, no. 5, pp. 349–355, May 2002.
- [13] Mr. Vikas Tigay, "have proposed "Data Hiding in Image using least significant bit with cryptography," International Journal of Advanced Research in Computer Science and Software Engineering

BIOGRAPHY



T.Muthu Lakshmi graduated B.E in Computer Science and Engineering from PET Engineering College, Vallioor, Tamil Nadu, India in 2014. Currently she is pursuing Master of Engineering in Manomaniam Sundaranar University. Her research interests in Digital Image Processing.



P.Mohamed Fathimal received her BE and ME in Computer Science and Engineering from Manomaniam Sundaranar University, Tirunelveli, Tamilnadu. She has 10 years of Teaching Experience. Currently She Is pursuing PhD in Manomaniam Sundaranar University. Her research interests include Digital Image Processing and Network Security.



Dr. P. Arockia Jansi Rani graduated B.E in Electronics and Communication Engineering from Government College of Engineering, Tirunelveli, Tamil Nadu, India in 1996 and M.E in Computer Science and Engineering from National Engineering College, Kovilpatti, Tamil Nadu, India in 2002. She has been with the Department of Computer Science and Engineering, Manomaniam Sundaranar University as Assistant Professor since 2003. She has more than ten years of teaching and research experience. She completed her Ph. D in Computer Science and Engineering from Manomaniam Sundaranar University, Tamil Nadu, India in 2012. Her research interests include Digital Image Processing, Neural Networks and Data