Unified Approach to Feature Extraction and Information Security for Image Processing Systems

Kaushik Subramanian
Waran Research Foundation
46-B, Mahadevan Street, West Mambalam
Chennai-600 033, India
kaushik@warftindia.org

Abstract

This paper aims at evolving a novel approach for feature learning and information security by unifying Image Processing techniques and Image Encryption. Enhanced images are processed by edge detectors followed by segmentation using the Radon transform. These characteristics are then transformed to a multi-dimensional space using the Gabor Transform to obtain the required feature vector. The uniqueness and the preservation of the image features is found to be maximum using this form of representation. Further the acquired vector is transmitted by using matrix-based encryption techniques. In this paper, the unification of the two is done using a common matrix environment. With the proposed Singular Value Decomposition and Partition methods of encryption, the problem of pixel randomness is overcome as it requires the transmission of only the encoded feature vector. The unification provides a secure and accurate image transmission system.

1. Introduction

During the last 20 years, Image Processing Systems have made considerable growth. The two most common methods currently employed are structural methods (character recognition, contour analysis) and feature space methods, the latter being more efficient. Feature Space Pattern Recognition involves a set of measurements made on a real world entity followed by the corresponding feature extraction based on these measurements to characterize the class of shapes and patterns obtained.

This form of Information Learning therefore requires an accurate recognition and classification of the image. This process has made great progress using Bayesian classifiers and decision trees. But when the system information is of higher orders, the image is covered by noise, and patterns are confused with each other or incomplete, image based modeling is very difficult. For solving some of these noise and feature extraction problems, this paper proposes a new feature learning algorithm.

Following the process of image enhancement and processing, the next step is to relay or transmit this information to a remote location in a secure manner. The proposed system converts the image into a feature vector space and it is found that this information is sufficient to reproduce the entire image at the receiver. The problem arises from the secure transmission of this vector. Multimedia communication systems such as Medical Imaging, Military Navigation and Satellite Information that transmit feature vector image matrices are often intercepted by unauthorized personnel. Although several conventional algorithms such as RSA and AES exist, they find limited application to images because of the large image size and complexity. To overcome these shortcoming; Determinant, Kernel and Singular Value Decomposition based methods have been evolved.

The paper is organized as follows. In section 2, Image Enhancement using statistical methods is explained. Section 3 deals with the Novel Feature Learning Algorithm and Section 4 deals with Image Encryption Matrix Algorithms. The Conclusions are presented in Section 5.

2. Image Enhancement Using Bootstrapping Filters

A complete image processing system consists of a sensor that gathers the observations to be classified or described; a feature extraction mechanism that computes numeric or symbolic information from the observations; and a classification or description scheme that does the actual job of classifying or describing observations, relying on the extracted features.

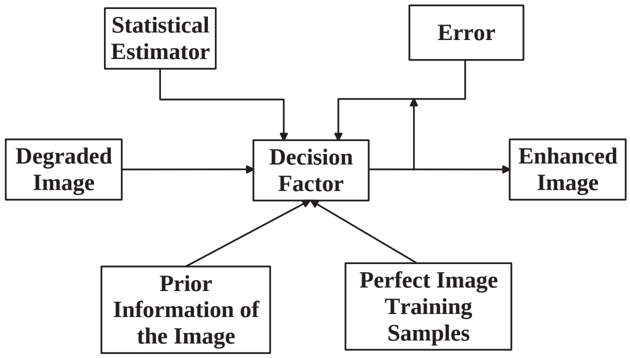

Figure 1. Image Enhancement using Bootstrapping Statistics

The accuracy of this System is increased by performing pre-processing operations such as Noise filtering. The Bootstrap Filter acts as a Non Linear Estimator. It acts on the random image samples and produces the target probability distribution function. The samples are then propagated and updated recursively. The advantage of using the Bootstrap Filter is that it is amenable to implementation on parallel processors and avoids the exponential estimation condition.

We know that the Image data collected by a sensor suffers from quality degradation. A good quality image should display shape edges at physical surface boundaries, and show smooth gradual intensity change on the physical surfaces. Such an image would allow edge information to be extracted unambiguously by the human eye or by an automated system. The most common kind of image degradation is the additive noise represented by the following equation.

$$x(i,j) = x_o(i,j) + n(i,j) \tag{1}$$

where
$x(i,j)$ is the intensity at pixel location (i,j)
$x_o(i,j)$ is the noiseless (ideal) pixel at (i,j)
$n(i,j)$ is the random noise

The Noise reduction filter will attempt to estimate $x_o(i,j)$ given $x(i,j)$. The better the filter, the closer to the ideal noiseless value its estimates are. Such noise reduction filters are usually some form of low-pass filter that smooth out noisy spikes in the data. However, they also lose some of the subtle edge information. Therefore, the trade-off is usually between smoothing and edge preservation. We find that the bootstrap mean filter reproduces the noiseless pixels more closely and also preserves more of the edge information. The system information flow is shown in Fig 1.

Using the training sample data, knowing what the perfect image should look like, the estimated parameters were used to gauge the performance of the filters. For measuring the restoration of the degraded image, the root-mean-square of the difference between the noisy image and the ideal image were calculated and compared as follows:

$$RMS = \sqrt{\sum_{i=1}^{row}\sum_{j=1}^{col}(x(i,j) - x_o(i,j)^2)/row * col - 1} \tag{2}$$

A smaller value here indicates that the filter does a better job in restoring the noisy pixels to match the ideal image. An often contradicting measure of filter performance is edge preservation. Most restoration is performed by applying a smoothing filter, which tends to wash out the edge information that is important in Pattern Recognition and Computer Vision applications.

3. Image Indexing And Feature Learning

The concept of Algorithm Level Encoding (ALE) is employed for Edge Detection. Once the process is complete, it is necessary to segment the image based on the computed edges. The Radon Transform functions in tune with the Contour Detector to perform a Region Based Segmentation of the enhanced Image. The processed image is then transformed to a multi-dimensional space using the Gabor elementary functions.

3.1. Using Algorithm Level Encoding for Edge Detection

Edges in an image can be detected by analyzing sharp patterns in the pixel values. But the difficulty lies in detecting these patterns in the image. Any pixel by pixel method of detecting them will be cumbersome. The ALE is found to be useful in this regard. We partition the image matrix into sub-matrices and subsequently compute their Checksum Rows and Columns.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \tag{3}$$

After ALE

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 7 \\ 4 & 6 & x \end{pmatrix} \tag{4}$$

In the provided example, the third row and third column represent the checksum row and checksum column respectively.
The ALE can applied to a block of pixel values by windowing it across the image. The checksums of this window and that of the corresponding image blocks are compared and

Figure 2. Top Row - Original 512 x 512 image, Edge Detected Image, Enhanced Image. Bottom Row - Segmented Image

any sudden increase or decrease in the pixel values indicate the presence of an edge. The windowing can be skipped if it is found that the checksum values do not show an appreciable change, when performed on a couple of blocks. The ALE algorithm can be made use of effectively for image enhancement purposes too. First, the edges are detected, using the ALE as explained. This can be done in a non-uniform manner. Subsequently, the boundary pixels so obtained can be analyzed and separated from the relatively unimportant aspects of the image. Since, the encoding is selectively done depending upon the criticality of the bootstrapped image, the decoded image can be claimed to be noise free. This is followed by a stage that can distinctively separate out the image edges and can aid in image segmentation. The edge detection operation can be viewed as inherent preprocessing technique of the image analysis system. This method will prove to be vital for the unification process of the image processing techniques.

3.2. Shape and Pattern Formation - Enhanced Image Segmentation using Radon Transform and Contour Analysis

The generalized Radon transform is a well-known tool for detecting parameterized shapes and patterns in an image. Given a model of the shape, it defines a mapping from the image space onto a parameter space. The axes of the parameter space correspond to the parameters of the model. When applied to the edge detected image, the Radon transform yields a Parameter Response Function (PRF) defined on the parameter space. A shape in the image becomes a peak in the PRF. The location of the peak corresponds to the parameters of the shape. Shape detection is thus reduced to peak detection.

We use the two common approaches to the discretisation of the Radon transform. The first is a straight-forward discretisation of the integral using standard numerical algorithms. It chooses a point in parameter space and computes its value by integrating the image over all the points belonging to the curve. In the second algorithm we choose a point in the image and add its contribution to all the appropriate points of the PRF. In its most general form, the Radon transform is

$$P(p) = \int_R C(p,s)I(s)ds \tag{5}$$

with $P(p)$ the PRF, $I(s)$ the image and $C(p,s)$ the shape for parameter vector p.

$$C(p,s) = K((p/x), x - s) \tag{6}$$

It follows that both the operator function C and the image $I(s)$ must be bandlimited to allow discretisation. Proper sampling of the edge detected image I is a prerequisite for any image analysis. We must impose a band-limit on C. The alternative, sampling C without imposing a band-limit first, leads to aliasing effects.

An advantage of the Radon paradigm is that it gives us control over how we visit the points in parameter space. On scanning through the entire image, we apply the equation 5 and 6 to obtain the Parameter Response Function.

Following this process of scanning using the Radon Transform, the Contour Detector is used to provide a fairly smooth distance measure between any two detected shapes, also regarded as contours. It is used to match the obtained shapes to the templates already present in the database. This technique if found to be tolerant to considerable misalignment in position, scale and rotation. This makes it perfect for our task of matching small rigid templates somewhat invariantly against a wide variety of images for the process of Image Segmentation. Fig.2 shows the results of the proposed techniques on a 512 x 512 grayscale image. In its simplest form, matching takes two sets of transformed images, the edge map of an image, $P(p)$, and the template (contour fragment), $T(t)$. Using the variables the Contour Detector evaluates the Matching score as a function of relative position x:

$$d_{T,P}(x) = 1/N_T \sum_t min(t+x) - p \tag{7}$$

where N_T is the number of segments in T. This gives the mean distance of edges in the template to their closest edges in the edge map. It can be efficiently computed by first evaluating the distance transform (DT) of the edge map. Each pixel in the DT is the distance to the closest pixel in the edge map finally computing the segmented image along with the matched shapes and patterns.

3.3. Gabor Elementary Functions for Feature Extraction

After the segmented signal is obtained, a windowed spectrum of the image is plotted and the corresponding dB levels are stored. An inverse Fourier Transform is performed on the stored data and the time-frequency expansion is initialized. The absolute value of the coefficients obtained are scaled and plotted. For a particular input image, the plot reveals a unique sequence of spikes. The feature vector set for the proposed system consists of image dominant vectors and associated eigen components.

$$F_v = [\delta; \lambda] \tag{8}$$

4. Unification Of Image Encoding and Encryption

A general class of cryptographic algorithms are employed mainly to exploit the properties associated with matrices. These matrix algorithms based approach provides a base for the unification of the aforementioned image processing techniques.

4.1. Evolution of Novel CryptoSystems using Matrix Algorithms

Most of the encryption system research work aims only at permuting the pixel arrangements and thereby attempting to disorient the image thereby providing randomness. However such CryptoSystems have not sustained for long and analysis has been reported that is vulnerable to known encoded image attacks. This paper provides encryption of a different kind, that differs from the existing methodologies by involving matrix related algorithms. These algorithms are chosen to exploit to the maximum, the characteristics associated with each matrix. The extraction of these unique set of data, lies entirely in the nature of the matrix algorithm used. It is found that the entire image can be regenerated from the encoded feature vector obtained from the Gabor Elementary Functions. Based on these results different general matrix algorithms based image CryptoSystems have been introduced. All of these algorithms differ in their ways of exploiting the set of unique parameters, associated with the images and the computed feature vector.

4.2. Determinant Method (DM) Based Matrix CryptoSystems

A matrix is randomly generated whose determinant satisfies a given value. Encryption is done by multiplying the feature vector with this random matrix. This forms the encoded key whose entries are largely decided by the selection of random matrix. The determinant value comes from additions of repeating factors of the random matrix. The factors involved are not restricted to only integers, but includes a mix of both integers and decimals values. Therefore predicting the image values by brute force method is highly impracticable, for it requires a complexity of $O(NXN!)$. The advantage of this method is that, even if the features are known to the attacker, it will still be difficult to arrive at the matrix without the proper setting of the random matrix entries, for they may exist several possible combinations of matrices whose determinant value matches the value of the encoded key. This property adds to the security of the proposed algorithm. The DM based Image transformation is shown in Fig 3. Decryption process is easily performed on the encoded key by taking the inverse of the feature vector matrix.

Redundancy is greatly reduced as every encryption process involves a different determinant number and a different set of matrix entries. Even if the determinant value repeats, the matrix entries differ widely, and this does not provide any scope for predicting the image patterns associated with the encoded key. The algorithm for arriving at the determinant value, involves the generation of a random matrix and subsequently perturbing the entries to converge onto this specified determinant value. Through this, the values of all the entries are dispersed relative to the determinant value, thereby inherently inducing randomness.

4.3. Partition Method (DM) of Encryption

Every three pixel across the rows of the enhanced image are replaced by their sum and their sum of the squares. For encryption, the sum is retained as σ and the image of the sum of the squares is transmitted as a code vector key. Any attempt to eavesdrop would not help without the sum of the pixels σ. For decryption, any three numbers are randomly generated and are reverse iterated so as to satisfy their sum and sum of their squares. This result may be be accurate but is definitely sufficient enough to reconstruct the image.

4.4. Singular Value Decomposition (SVD) Based Image Encryption and Compression by Jacobi Transformation

The SVD decomposition by Jacobi Transformation technique proves to be an important tool for the proposed image CryptoSystems. This is based on a code vector management system, which further adds security to the CryptoSystems. The rotation angles of any vector in space is transmitted across the channel as code vector and its associated eigenvalues are retained as the feature space. Further sections are dedicated to the SVD based encryption approach. The SVD algorithm is first described and later encryption/decryption processes are presented.

4.5. The Algorithm

This section deals with description of cyclic SVD based on Jacobi Transformation. For a 22 orthogonal matrix

$$J = \begin{pmatrix} c & s \\ -s & c \end{pmatrix} \tag{9}$$

Where$c = cos(x)$ and $s = sin(x)$ The computation of the image matrix X is a two step process involving

1)Symmetrisation
2)Diagonalization

Symmetrization
The image matrix X is first transformed into a symmetric matrix Y by pre-multiplying it with the transpose of a Jacobi plane rotation. This is given by

$$J^T X = Y \tag{10}$$

The J matrix can be computed knowing either $X or Y$ matrix.

Diagonalization
The matrix Y is symmetric. Y can be diagonalized by pre-multiplying and post-multiplying by the transpose of a jacobian matrix and the jacobian respectively. Here J_2 is the Jacobi matrix to be determined.

Figure 3. a.Original 256 x 256 Lenna Image, b. DM Encrypted, c. SVD Encrypted

$$J_2^T Y J_2 = Z \tag{11}$$

where Z is the diagonal matrix. SVD for a general square matrix is computed by solving appropriate sequence of $2x2$ SVD problems. In SVD encryption, we transmit only the rotation angles of the matrix J_2 and J as the code vector, and the eigenvalues of the Y are embedded in J_2. The CryptoSystems is secure from the point of view that only a factor of the image is transmitted, whose sole knowledge does not provide the attacker with the contents of the original image. The results of the SVD Encryption Algorithm are shown in Fig3. The rotation angles of J_2 are kept private. At the receiver end, the image matrix X is found out by using the rotation angles of the left and the right eigenvectors.

4.6. Unification of Image Processing Techniques, Encoding and Encryption

As a final step , the unification of all the image processing techniques is accomplished as shown in Fig 4. The uni-

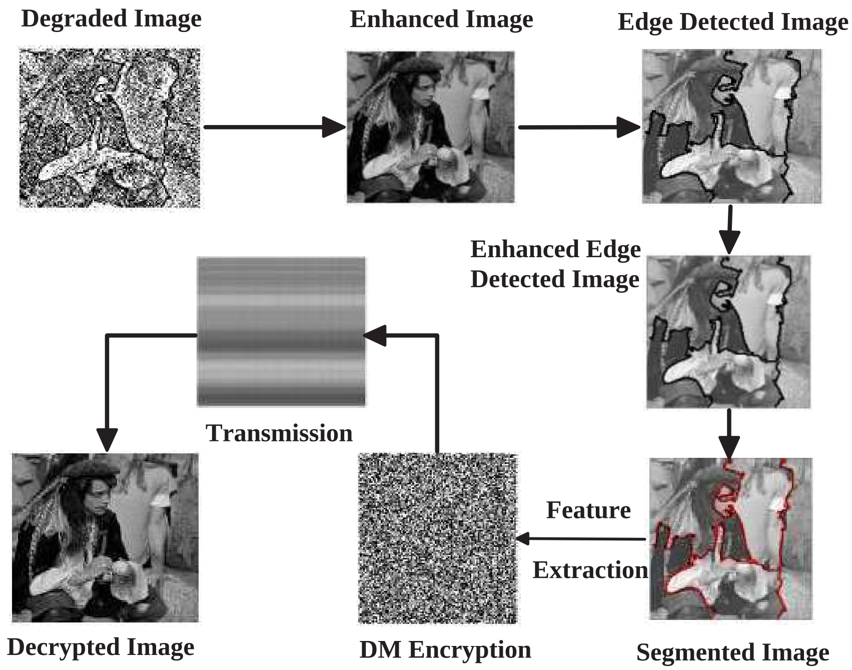

Figure 4. Unified Pattern Analysis System

fication is easier to come by, due to the presence of a common base - Matrix characteristics and related operations. This unification includes image enhancement, edge detection, image encryption and segmentation.

5. Conclusion

The proposed approach, exploits the properties associated with matrices in unifying Image Processing techniques and Encryption. This was possible because of the transmission of image factors instead of harping on permuting the matrix entries for data encryption. Further reliability of the image transfer is preserved through encoding it into a Multidimensional Feature vector set. With this unification as a base, an Image Analysis and Encryption System can be evolved comprising of all the techniques required to maintain the security and quality of the image.

References

[1] Neil Gordon. "A Hybrid Bootstrap Filter For Target Tracking In Clutter" *IEEE Transactions, Defence Research Agency*, 1997.

[2] Chandni Patel, T. Srikanthan and Sangeetha Narayan. "A Rotation-invariant Embedded Pattern Recognition System" *IEEE ICIT02*, Bangkok, THAILAND, 2002

[3] Andrea Cavallaro. "Image Analysis And Computer Vision For Undergraduates" *ICASSP '05*, V:577–580, 2005.

[4] A. K. Jain. "Fundamentals of Digital Image Processing" *Prentice Hall*, 1988.

[5] S. Agarwal and D. Roth. "Learning A Sparse Representation For Object Detection" *In Proc. ECCV*, page IV: 113 ff., 2002.

[6] R. Mayer, J. Edwards and J. Antoniades. "Segmentation Approach And Comparison To Hyperspectral Object Detection Algorithms" *Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05)*.

[7] Jamie Shotton, Andrew Blake and Roberto Cipolla. "Contour-Based Learning for Object Detection" *Proceedings of the Tenth IEEE International Conference on Computer Vision (ICCV05)*.

[8] Shujun Li, Chengqing Li,Guanrong Chen, Dan Zhang,Nikolaos G. Bourbakis. "A General Cryptanalysis Of Permutation-Only Multimedia Encryption Algorithms" *Cryptology - ePrint Archive* 2004.