Asian Journal of Information Technology 15 (17): 3182-3195, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Attack Resistant Analysis Using Secure Singular Value Decomposition and Markov Random Field Based on Rotation Scaling Transformation Invariant Image Watermarking for Video Frames

[1]S. Poongodi and [2]B. Kalaavathi
[1]Department of ECE, K.S.R. College of Engineering
[2]Department of CSE, K.S.R Institute for Engineering and Technology,
Anna University, Chennai, Tamil Nadu, India

Abstract: This research proposes a novel video watermarking model for video frames based on Rotation Scaling Transformation (RST). Most of the available watermarking methods utilize image processing techniques to execute the watermarking task. This proposal adopts a K Dependency Bayesian (KDB) Model for the approximation of the frames according to probability values. In the study presented, video frames are segmented using the Markov Random Field (MRF) segmentation technique where KDB represents every part of the frame region. Singular Value Decomposition (SVD) is used for encryption of the selected feature points. The encrypted areas located at the feature points are utilized for watermark embedding and extraction. During the stage of embedding, the text files are converted into a matrix. Both the matrices are then merged using the sum of the matrices. The watermark embedding strength is adapted according to the noise visibility function and the analysis of the probability of error is performed mathematically. Simultaneously, the watermark embedding and extraction techniques are assessed based on a proven mathematical model. Experimental results prove that the proposed MRF-SVD video watermarking method performs better in terms of invisibility and robust behavior in comparison to the previous methodologies under potential attacks such as cropping, rotation, scaling, sharpening and Gaussian noise in case of videos.

Key words: Rotation Scaling Transformation (RST), K Dependency Bayesian (KDB) Model, Marko Random Field (MRF) segmentation technique, Singular Value Decomposition (SVD), watermark embedding and extraction techniques

INTRODUCTION

The fast growth of new information methodologies has enabled easy access to digital information. On the other hand, it has also worsened the issue of illegal copying and redistribution of digital media. The technique of digital watermarking was introduced when there were attempts made to resolve issues in relation to the intellectual property rights of media management. A digital image watermarking scheme must be effective enough to tackle a variety of potential attacks. Geometric distortions pose more difficulty in thwarting in comparison to other types of attacks. The technology of digital watermarking was put into application when trying to resolve the troubling issues associated with the management of intellectual property of digital products (Zheng *et al*., 2007).

A watermark is a digitized code which is implanted into the digital cover content i.e., text, audio or video sequence. Digital video is basically a collection of sequential still images. A watermark can be used to carry any kind of data but the amount of the data that it can carry is limited. The amount of information that can be embedded into the video is referred to as payload. The level of vulnerability of information increases in proportion with the amount of the information a watermark carries. Again, the amount of information that a watermark can carry is purely restrained by the size of a specific video sequence. Watermarking gives more preference to robustness rather than capacity. Hence, a watermark basically carries tens to thousands of concealed data in bits per video frame (Jayamalar and Radha, 2010).

Digital watermarking is found to be an efficient solution to the issues of multimedia video frames and data authentication. Myriad of geometric invariant algorithms have been put forward in the last few years (Zheng *et al*., 2007). Digital image watermarking technologies can be classified into three important categories: implanting the

Corresponding Author: S. Poongodi, Department of ECE, K.S.R. College of Engineering, Anna University, Chennai, Tamil Nadu, India

watermark in the geometric invariant domain (Zheng *et al*., 2007); implanting a template along with the watermark (Zheng *et al*., 2007) and implanting the watermark on the basis of feature selection techniques which in the recent times has shown good performance with respect to robustness (Seo and Yoo, 2006; Zheng *et al*., 2009).

A strategy for the detection of watermarks after geometric distortion is the identification of the distortions and the application of inverse transform before watermark extraction. This can be performed by embedding a template along with the watermark (Fouda, 2015) into the cover image. Researchers have proposed embedding of two watermarks, a template and a spread spectrum message which contains the information or payload. The template comprises no data by itself but is utilized for detection of the transformations made to the watermarked image. This type of template is suitable for all images. However, it has the limitation of being easy to remove as the template generally corresponds to peaks in a transform domain. This fact may increase conniving attempts to reveal the registration pattern and, after its discovery; the removal of registration pattern from the watermarked image could be done, thus posing a restriction on the reversible capability of any geometric distortions.

Nowadays, most of the watermarking schemes exhibit poor performance against geometrical attacks. The general geometrical attacks are rotation, flipping, translation, aspect ratio changes, resizing and cropping. Watermarking schemes apply several synchronization techniques for handling geometrical attacks. These approaches generally attempt to identify the geometrical distortions and reverse them before the watermark detector is made use of. The identification of the geometrical distortions is accomplished by the examination of a registration pattern embedded along with the watermark in the host image (Coria *et al*., 2007). However, the addition of the registration pattern to the data-carrying watermark decreases the fidelity of the watermarked image in addition to the scheme's capacity. Another drawback of this technique is that, generally all the watermarked images carry the same registration watermark. Hence, it is an easy task to detect the registration watermark through illegal attempts. Once the registration pattern is found, it could be removed from all the watermarked images, thus limiting the chances of the invertibility of any geometric distortions. In addition, these techniques increase the computational time considerably and in few cases their performance is poor. This issue is resolved by using the feature points based watermarking scheme which again performs the detection of the attacks against geometric properties.

Recently researches have put forward a digital video watermarking scheme (Yuan and Pun, 2013) which is efficient to geometric distortions, such as rotation, scaling and cropping. The embedding/extraction of the watermark is based on feature selection and local Zernike transform in/from each selected frame. The feature selection technique called Adaptive Harris Detector which follows the revised traditional Harris Corner Detector and the local Zernike moments-based technique is used for watermarking. In each selected frame, the selected circular patches are broken down into a collection of binary patches with Bit-Plane Decomposition method. It has been established that the selected feature points can subsist a wide range of attacks and can be used as reference points for both watermark embedding and extraction. Results obtained from experiments show that the performance of the watermarking technique is not up to the mark against sharpening and noise in the attack. It can also be inferred from these experiments that the removal of feature point's noise is not performed precisely, if the watermarked image undergoes distortions and geometrical transforms. Significant improvement cannot be obtained even with higher order moments calculation.

A new video watermarking technique was proposed on the basis of the rotation invariant feature and image normalization to resolve the problems quoted above. The K-Dependence Bayesian (KDB) image segmentation technique has been applied for segmentation of the video frames image into several homogeneous areas. One feature point is selected using Markov Random Field (MRF) for each region. These points are strong against rotation, scaling and cropping. Rotation of the area is done for every feature points disk, to align it with the feature point. Then image normalization is used to transform the disk region to its compact size which is scale invariant. After the rotation and scaling of video frame samples, the encryption of video frame content is done using Singular Value Decomposition (SVD). Using these techniques, the security of video content is assured, watermark embedding and extraction is done. In watermarking embedding stage the encryption of the snapshots and text file of the question paper to video frames is performed, then attack resistance is conducted for embedded watermarked video frame image. A mathematical model is very important for the analysis of the watermarking process. The estimation of KDB parameters is done using MRF. The adaptive adjustment of the quality of the embedded video watermarked image samples is done based on the characteristics of the embedding region, by using noises. The results are figured based on the PSNR and MSE.

Literature review: Mirza *et al.* (2007) have suggested a digital video watermarking approach based on Principal Component Analysis (PCA). An undetectable watermark is embedded into the three different RGB channels of the video frame using PCA transform in isolation. The chief advantage of this technique is that the same or multi-watermark can be implanted into the three color channels of the image for increasing the robustness of the watermark. The usage of PCA transform helps in the choice of the desirable substantial components into which to embed the watermark. The results from previous experiments demonstrate a high degree of reliability against the general video attacks, especially frame dropping, cropping and rescaling for a good quality perception.

Al-Taweel and Suma (2009) have introduced a new DWT-based video watermarking algorithm on the basis of a three level DWT making use of Haar filter which is again efficient against geometric distortions such as Downscaling, Cropping and Rotation. It is also very reliable against image processing attacks such as Low Pass Filtering (LPF), Median filtering and Weiner filtering. Moreover, the algorithm is strong against Noise attacks such as Gaussian noise, Salt and Pepper attacks. The embedded data rate is high and it is less prone to attacks. It has been observed from the experimental results that the embedded watermark is hard and not seen.

Mostafa *et al.* (2009) presented a new method for a binary logo watermark embedding into video frames. Discrete Wavelet transform is performed on every video frame. PCA is then applied to each block of the two bands (LL-HH). The watermark is embedded into the principal components of the LL blocks and HH blocks in many ways. The test results depict that there is no easily observable difference between the watermarked frames and the original frames and show the efficiency against a wide range of attacks such as MPEG coding, JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, contrast adjustment, sharpen filter, cropping, resizing and rotation. Combination of the two transforms help in the improvement of the performance of the watermark algorithm.

Bhatnagar and Raman (2012) introduced a Wavelet Packet Ttransform (WPT)-based robust video watermarking algorithm. A visible comprehensive binary image is used as the watermark. In the first stage, frames in sequence are extracted from the video clip. The WPT algorithm is then employed on each frame and from each orientation, selection of one sub-band is done on the basis of block mean intensity value called robust sub-band. The embedding of Watermark is done in the robust sub-bands according to the relationship between wavelet packet coefficient and its 8-neighbour (D8) coefficients taking into consideration the robustness and invisibility. Experimental results prove the robustness and the better performance of the algorithm and in comparison with other available algorithms in the literature.

A real-time video watermarking technique (Wang *et al*., 2011) against geometric distortions has been suggested for DCT-encoded compressed video data. The full DCT coefficients have been established to be unvarying to scaling and local geometric attacks. Hence, watermarks are embedded into Watermark Minimal Sequences (WMS) by the modulation of the low-frequency full DCT coefficients. To satisfy the needs of real-time performance, a fast inter transformation is applied for the construction of full DCT obtained directly from block DCTs. The changes of full DCT coefficients are applied to inverse transformation of the differences of block DCT coefficients that are added in subsequent steps to the original block DCTs for the generation of the WMS. The technique can withstand rotation attacks with the employment of a rotation compensation strategy.

An adaptive blind video watermarking technique (Park *et al*., 2006) using video characteristics according to the Human Visual System (HVS) in three-dimensional discrete cosine transform (3D-DCT) domain has been proposed. The patterns of 3D-DCT cubes and the types of video segments are classified for the optimization of the weight factors for watermarking. Classification utilizes the texture and motion information of 3D-DCT cubes. An optimized watermark is embedded into the mid-range coefficients of 3D-DCT cubes with the help of trained optimal weight factors. The results obtained from experiments prove that the proposed method offers good performance in the presence of various potential attacks such as MPEG compression, frame dropping, frame insertion and frame swapping with respect to invisibility and robustness than the techniques in prevalence before.

A new robust video watermarking system on the basis of Hidden Markov Model (HMM) and Artificial Neural Network (ANN) (Elbasi, 2007) has been developed. The suggested watermarking approach splits the video sequences into Group of Pictures (GOP) with HMM. Parts of the binary watermark have been embedded into each GOP with a chosen transformation domain watermarking algorithm. ANN constructs the optimal transformation algorithm for each corresponding GOP. The embedding procedure is the standard additive algorithm in low and high frequencies in varied transformation domains.

MATERIALS AND METHODS

Proposed video file is secured using SVD with markov random field watermarking scheme and attack resistant analysis: This research work introduces a new attack tolerant analysis schema for video watermarking image. Initially the video file is given as input for the original

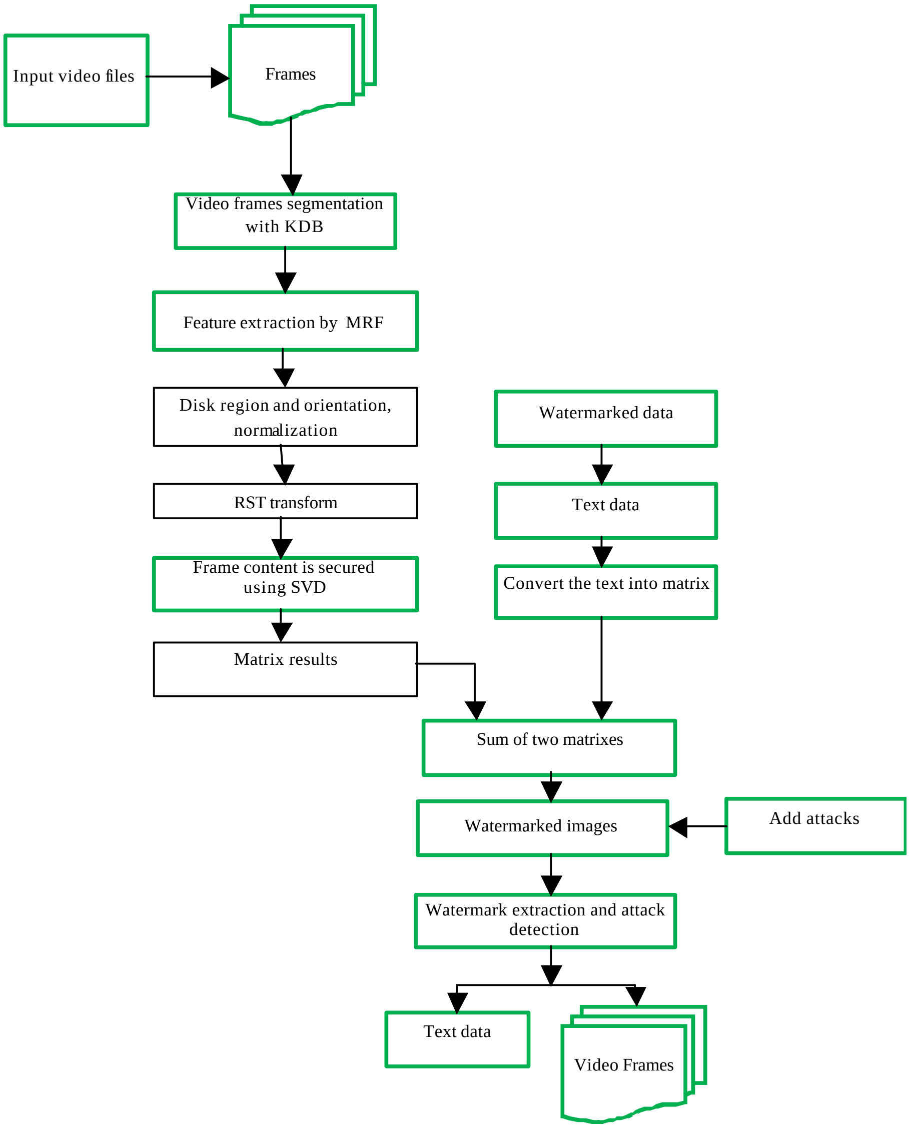
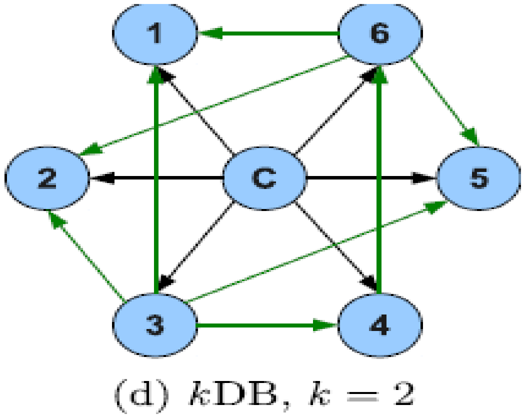

Input video files
Frames
Video frames segmentation with KDB
Feature extraction by MRF
Disk region and orientation, normalization
RST transform
Frame content is secured using SVD
Matrix results
Watermarked data
Text data
Convert the text into matrix
Sum of two matrixes
Watermarked images
Add attacks
Watermark extraction and attack detection
Text data
Video Frames

Fig. 1: Architecture of the proposed system

image. The conversion of video files into frames takes place next. Random selection of any one frame in the video file is done, then the frame is segmented into a number of homogeneous parts and the feature points are selected. The frames in the video files are segmented on the basis of K-Dependence Bayesian (KDB). The circular areas for watermark embedding or extraction are then determined. The rotation, scaling and translation invariant areas can be used for watermark embedding and extraction on the basis of the image normalization and orientation assignment. The segmented image is simulated as Markov Random Field of mathematical analysis for various features of the watermarking processes such as embedding strength adjustment. Encryption is done to provide more security to video frames. Encryption is done using the Singular Value Decomposition (SVD). The encrypted output is given as input to the watermarking process. There are four important parameters which are generally utilized for the determination of the quality of the watermarking scheme. They are robustness, imperceptibility, payload and security. Robustness is defined as the measure of resistance of watermark, against attempts to image modification and manipulation like filtering, rotation, scaling, resizing, cropping, etc. Methods such as filtering, rotation, scaling, sharpening, cropping are used to perform attack detection for watermarked video and text data. Question papers with text files (Snapshot of the question paper) are considered as watermarked images. The proposed architecture is illustrated in Fig. 1.



(d) kDB, $k = 2$

Fig. 2: The K-Dependence Bayesian (KDB) classifier

A simplified mathematical representation of video frames suggested has been suggested in (Rubio and Gamez, 2011). Cox's method uses spread spectrum communication techniques to embed the watermark in the image as shown in the following equation:

$$Y = VF + \times W \tag{1}$$

Where the original frame of the video is estimated as a communication channel. The watermark W is considered as a signal to be transmitted in the channel. The embedding strength, gives the amplification or reduction of the power of the signal. In this technique, the video frame is simulated using Markov Random Field (MRF). The video frame is segmented into much similar regions using K-Dependence Bayesian (KDB) image segmentation (Fig. 2). Each area is simulated using MRF. The pixels in each area have alike statistical features. Several issues like false positive probability and watermark embedding strength can be deduced mathematically with this model, rather than proving experimentally.

K-Dependence Bayesian (KDB) for frames segmentation: Segmentation is the procedure of division of the video frame VF samples into video frame areas and the representation is given as VFOR. In recent times, several research works have been conducted with the use of Bayesian network for classification jobs. Hence, it is used for image segmentation for videos or images. The visible video frame results are represented as VFOR and the segmentation is given by VF, for each subregion VF_s of the segmentation. Since it computes approximate posterior probability value (c^*) for each video frame region, it is applied to images video frame predictor observed values. The likelihood is then given by:

$$p(VF_s \mid VFOR_s) = p(VF_s \mid VFOR_s)p(VF_s) / p(VFOR_s) \tag{2}$$

$$\begin{aligned} & VFOR^* \\ & = \underset{vfor}{\arg\max} P\left(VFOR = vfor|VF_S = vf_1,\ldots,vf_n,\theta\right) \\ & = \underset{vfor}{\arg\max}\, \rho\left(VF_1 = vf_1,,,VF_n = vf_n,\omega|VFOR = vfor\right) = vfor \end{aligned}$$

Noting that $p(vs_i)$ does not depend on the labeling vfor, we have,

$$\rho(vf_1,\ldots.Vf_n \mid vfor) = \prod_{i\in s} \rho(vf_i,\theta \mid vfor) \tag{3}$$

Where $\rho(vf_i,\theta \mid vfor)$ denotes the θ degree of sparsity with maximum likelihood of video frame predictor observed values $vfor_i$ for known video frames sub regions, vf $_i$it captures information about. In the usual Bayesian learning technique, the probability values are computed on the basis of conditional independence function between video frame predictor observed values ($VFOR_1$,...$VFOR_n$) and their values are obtained from the Cartesian product. It becomes a presumption as time passes by. Data with k-Dependence Bayesian (kDB) classifier (Rubio and Gamez, 2011) is additionally considered for solving the assumption problem in Bayesian learning techniques. It is an extension f basic Naive Bayes classifier with number of parents for each set of video frame predictor observed values. Navie Bayesian classifier is also defined as Markov Blanket (MB) for videos or images. Each and every Markov Blanket (MB) of class variables indicates the exact video frame predictor observed values for each video frame and their sub areas:

$$P\left(VFOR|VR_1,\ldots,VR_n,\theta\right) = P(VFOR \mid MB\left(VFOR\right)) \tag{4}$$

The most important property of this K-Dependence Bayesian (KDB) is that MB, a video frame sub region of is conditionally independent of all video frames.

Markov Random Field (MRF) for salient feature detection: In this research, the MRF method uses the Difference of Gaussian (DoG) to perform the approximation. The result of the KDM segmentation information is used to locate of the geometrical-transform-invariant feature points which will be utilized as the reference for watermark embedding and detection. In this research work, the videos frame VF is a manifestation of the underlying video frames. Thus, the MRF salient feature extraction comprises of the hidden results from KDB segmentation and the observable noisy free video frames as VF. The goal of MRF is the discovery of salient features of video frames v for which increases the posterior probability, that is given by:

$$\mathrm{MRF}_{R^{NS}} = \arg\max_{\mathrm{VFOR}} P(\mathrm{VF}|\mathrm{VFOR})P(\mathrm{VFOR}) \quad (5)$$

P(VFOR) follows a Gibbs distribution:

$$P(\mathrm{VFOR})_{R^{NS}} = \frac{1}{z}\mathrm{expexp}(-U(\mathrm{VFOR})) = \frac{1}{z}\mathrm{expexp}(-\sum_{C\in c} V_c(\mathrm{VFOR}_c) \quad (6)$$

where, U(VFOR) is called an energy function, $z = \Sigma_{\mathrm{VFOR}}$ exp(-U(VFOR)) is the normalizing constant and V_c represents the clique potential for selected video frame . The feature points with strong edge responses will be eliminated due to their sensitivity to noise. Suppose that the original frame of the video is denoted as f(VF,VFOR) and the MRF blurred frame filtered by gaussian mr(VF,VFOR) filter defined in Eq. 5 is:

$$\mathrm{mr}_1(\mathrm{VF},\mathrm{VFOR}) = \mathrm{MRF}_{R^{NS}}\mathrm{MRF}_{R^{NS}} \times f(\mathrm{VF},\mathrm{VFOR}) \quad (7)$$

$$\mathrm{mr}_2(\mathrm{VF},\mathrm{VFOR}) = \mathrm{MRF}_{kR^{NS}}\mathrm{MRF}_{kR^{NS}} \times f(\mathrm{VF},\mathrm{VFOR}) \quad (8)$$

mr_1(VF,VFOR) and mr_2(VF,VFOR) are basically different from each other in scale by a constant factor K. Then, the DOG filtered video frame can be measured as follows :

$$\begin{aligned} \mathrm{DOG} &= \mathrm{mr}_2(\mathrm{VF},\mathrm{VFOR}) - \mathrm{mr}_1(\mathrm{VF},\mathrm{VFOR}) \\ &= \mathrm{MRF}_{KR^{NS}} * f(\mathrm{VF},\mathrm{VFOR}) - \mathrm{MRF}_{R^{NS}} * f(\mathrm{VF},\mathrm{VFOR}) \end{aligned} \quad (9)$$

With the result of frame segmentation, one feature point is selected for each segmented area and the circular region centered at the selected feature point with radius will be utilized for the watermark embedding and detection. In each segmented region, the selection of the feature point with the most number of pixels in its circular region which fits into the same distribution is done. Once the selection of reference feature points are done, the rotation and scaling invariant properties are assigned to the circular regions centered at the selected feature points.

Orientation assignment and circular region alignment: The orientation assignment (Lowe, 2004) is useful for making the circular regions rotation invariant. To do so, a window centered at the selected feature points is fixed. The gradients of all frames in the pixels in these windows are calculated using the first order derivative. The histogram of the gradient is then computed and the peak of the histogram is assigned as the orientation of the feature point. Hence, the orientation would not be disturbed by noise, small local distortion or some displacement of the feature point position. The gradient of pixel (VF_0,VFOR_0) in the video frame of V is computed as follows:

$$\nabla V(\mathrm{VF}_0,\mathrm{VFOR}_0) = \left[\frac{\partial V}{\partial \mathrm{VF}}, \frac{\partial V}{\partial \mathrm{VFOR}}\right]_{(\mathrm{VF}_0,\mathrm{VFOR}_0)} \quad (10)$$

The magnitude of this gradient is given by:

$$\sqrt{\left(\frac{(\partial V)}{(\partial \mathrm{VF})}\right)^2 + \left(\frac{(\partial V)}{(\partial \mathrm{VFOR})}\right)^2} \quad (11)$$

and it orientation is given by $\tan^{-1}((\partial V)(\partial \mathrm{VFOR})/\partial \mathrm{VF})$. The frame content from the probability distribution function results with RST orientation estimation content is made secure using the singular value decomposition. The suggested techniques can encrypt a frame based on SVD and it can be applied for both grayscale and colored frames, for color image same technique applied for each color band.

Step 1: The first step in this study is the creation of the needed keys for scrambling the frame feature point data which suggest three real keys which are created on the basis of the following relations which are decided by experiments:

$$\begin{gathered} [7 < \mathrm{Key}_1 < 10] \\ [0.9 < \mathrm{Key}_2 < 3\mathrm{and\,int}(\mathrm{Key}_2 * | 100) \neq 150] \\ [0 < \mathrm{Key}_3 < 3] \end{gathered} \quad (12)$$

Step 2: The frame values are scrambled using the according to the following relations:

$$\mathrm{FFP}_1 = \mathrm{Key}_1 \times \mathrm{Max}(\mathrm{AFFP}_1) - \mathrm{FFP} \quad (13)$$

$$\mathrm{FFP}_2 = \mathrm{Key}_1 \times \mathrm{Max}(\mathrm{FFP}_1) - \mathrm{FFP}_1 \quad (14)$$

Employ a scrambling process to the frames feature points (matrices) (FFP_1,FFP_2) for the conversion of their values to extremist values; the output of this step is two matrices (FFPE_1,FFPE_2) with extremist elements, one for the positives elements while the other is for the negative elements:

$$\mathrm{FFPE}_1 = \mathrm{FFP}_1 - \mathrm{FFP}_2 \quad (15)$$

$$\mathrm{FFPE}_2 = \mathrm{Key}_2 \times \mathrm{FFPE}_1 + \mathrm{FFP}_2 \quad (16)$$

Step 3: Apply SVD for both matrices resulting from the previous step (FFPE$_1$ and FFPE$_2$). Three matrices are obtained for each matrix from SVD:

$$[\mathrm{UFFPE}_1, \mathrm{SFFPE}_1, \mathrm{VFFPE}_1] = \mathrm{SVD}(\mathrm{FFPE}_1) \quad (17)$$

$$[\mathrm{UFFPE}_2, \mathrm{SFFPE}_2, \mathrm{VFFPE}_2] = \mathrm{SVD}(\mathrm{FFPE}_2) \quad \mathbf{(18)}$$

Step 4: Rebuild new matrix from the results of SVD process in step 3, this can be done by interchanging the singular values (SFFPE) of FFPE$_1$ with singular values of FFPE$_2$:

$$\mathrm{CFFP}_1 = \mathrm{UFFPE}_1 \times \mathrm{SFFPE}_2 \times \mathrm{VFFPE}_1^{\mathrm{T}} \quad (19)$$

$$\mathrm{CFFP}_2 = \mathrm{UFFPE}_2 \times \mathrm{SFFPE}_1 \times \mathrm{VFFPE}_2^{\mathrm{T}} \quad (20)$$

Step 5: For more complexes, the same steps above can be repeated for the creation of new matrices. Scrambling the elements in matrices (CFFP$_1$, CFFP$_2$) to get new matrices (DFFP$_1$, DFFP$_2$):

$$\mathrm{DFFP}_1 = \mathrm{CFFP}_1 - \mathrm{CFFP}_2 \quad (21)$$

$$\mathrm{DFFP}_2 = \mathrm{Key}_3 \times \mathrm{D}_1 + \mathrm{C}_2 \quad (22)$$

Then, SVD applied for both matrices (DFFP$_1$, DFFP$_2$) and replacement of the singular values of (DFFP$_1$) with singular value of (DFFP$_2$) is performed as stated in previous steps to get new matrices (EFFP$_1$, EFFP$_2$):

$$[\mathrm{UDFFP}_1, \mathrm{SFFPD}_1, \mathrm{VFFPD}_1] = \mathrm{SVD}(\mathrm{DFFP}_1) \quad (23)$$

$$[\mathrm{UDFFP}_2, \mathrm{SFFPD}_2, \mathrm{VFFPD}_2] = \mathrm{SVD}(\mathrm{DFFP}_2) \quad (24)$$

So that:

$$\mathrm{EFFP}_1 = \mathrm{UDFFP}_1 \times \mathrm{SDFFP}_2 \times \mathrm{VDFFP}_1^{\mathrm{T}} \quad (25)$$

$$\mathrm{EFFP}_2 = \mathrm{UDFFP}_2 * \mathrm{SDFFP}_1 * \mathrm{VDFFP}_2^{\mathrm{T}} \quad (26)$$

Step 6: Combine (EFFP$_1$ and EFFP$_2$) is one matrix:

$$\mathrm{F} = [\mathrm{EFFP}_1 \mathrm{EFFP}_2] \quad (27)$$

Step 7: This step is left with two different choices to combine (EFFP$_1$ and EFFP$_2$). Matrix values are converted into normalized values for reducing the complexity of the above step. Scaling normalization is applied to acquire the scaling invariance for the circular region. It makes the transformation of the image into its standard form by translating the origin of the image to its centroid. Feature scaling used to bring all values into the range [0,1]. This is also called unity-based normalization. This can be generalized to restrict the range of values in the dataset between any arbitrary points a and b using:

$$\mathrm{Fm}' = \mathrm{a} + \frac{(\mathrm{F} - \mathrm{F}_{\min})(\mathrm{b} - \mathrm{a})}{\mathrm{F}_{\max} - \mathrm{F}_{\min}} \quad (28)$$

with:

$$\mathrm{a} = \sqrt{\frac{ß?}{\mathrm{m}_{0,0}}}\mathrm{b} = \sqrt{\frac{ß}{?\mathrm{m}_{0,0}}} \quad (29)$$

Where:

a = The factors of the frame to one and they are defined by $\mathrm{al}_{\mathrm{VF}} = \mathrm{bl}_{\mathrm{F}}$

b = The factors of the frame to one and they are defined by $\mathrm{al}_{\mathrm{VF}} = \mathrm{bl}_{\mathrm{F}}$

l_{VF} = The height of the frame β and $\mathrm{m}_{0,0}$

l_{F} = The width of the frame β and $\mathrm{m}_{0,0}$

The zero order moment of f(VF/a), f(VF/b) and f(VF, F) and $\gamma$is the aspect ratio of the frame and is defined as $\gamma = \mathrm{l}_{\mathrm{F}}/\mathrm{l}_{\mathrm{VF}}$. The text files need to be converted into a matrix to performing the embedding process for the cover image matrix. Conversion of the text files into the matrix consists of the following steps : Consider the text file contains 2 sentences:

- This is very very nice picture
- The picture quality is nice

The file is converted into the following matrix format. The header line is all the common words in the text file. The second line represents the frequency of words in each sentence. The output matrix is:

$$\begin{bmatrix} 1\,1\,2\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1\,1\,1 \end{bmatrix}$$

This is very nice picture the quality. Then the watermarked text matrix and the frame matrix are combined into a single matrix.

Watermark embedding: The Noise Visibility Function (NVF) (Sajasi and Moghadam, 2013) describes the local features of the frame and offers a way to do the texture masking in spatial domain. The local variance for each segmented region is computed using NVF:

$$\mathrm{NVF}(\mathrm{VF}(\mathrm{i},\mathrm{j})) = \frac{\mathrm{h}(\mathrm{i},\mathrm{j})}{\mathrm{h}(\mathrm{i},\mathrm{j}) + \mathrm{s}_{\mathrm{s}}^{2}\mathrm{R}^{\mathrm{NS}}} \quad (30)$$

Where:

$$h(i,j) = \rho_s\left(?\left(\rho_s\right)\right)^{\rho_s} 1/\left|r\left(i,j\right)\right|^{2-\rho_s} \tag{31}$$

$$\eta\left(\rho_s\right) = \sqrt{\frac{\Gamma\left(\frac{3}{\rho_s}\right)}{\Gamma\left(\frac{1}{\rho_s}\right)}} \tag{32}$$

$$r\left(i,j\right) = \frac{x\left(i,j\right)-\mu_s}{s_s R^{NS}} \tag{33}$$

where, ρ_s is the shape parameter ranging from 0.3-2 for most of the frames in the video and μ_s, $\sigma_s R^{NS}$ be the mean and standard deviation for the selected region frame, respectively. The watermark embedding equation with NVF is given in Eq. 34:

$$F_s = VF_s + \left(1 - NVF\right).a.w \tag{34}$$

Where:

VF_S = The original video frame data in the circular region
α = The predefined embedding strength
w = The random watermark sequence which is developed under normal distribution and is the same size as one circular region

The watermark embedding procedure comprises of the following steps:

- Use the Pseudo random Number (PN) generator to yield a watermark text data sequence which is a spread spectrum consisting of both positive and negative values
- The adaptive embedding of the watermark text data into each of the selected circular regions is done using the following equation

$$f_s^{'}\left(VF,F\right) = f_s\left(VF,F\right) + [1 - NVF\left(f_s\left(VF,F\right)\right].a.w \tag{35}$$

Where:

$f_s(VF, F)$ = One of the circular regions of the original video frame
$f_s^{'}(VF, F)$ = The watermarked result, α is initially set as 2
S = The size of region

If the PSNR of the watermarked image is >40 dB, the watermark embedding is successful. Otherwise, α will be decreased by 0.1 iteratively until either of the following criteria is attained:

- The embedding strength is not bigger than 1.5
- The PSNR of the watermarked image increases to 40 dB

After completion of the process of watermark embedding, attack detection is conducted on the basis of attack resistant methods such as rotation, scaling, cropping, sharpening and filtering.

Rotation: It is also a type of attack. The image is rotated to 90° and tested. Once the reference feature points are selected, assignment of the rotation and scaling invariant properties to the circular regions centered at the selected feature points is done.

Scaling: It is the ability of a system, network or process to cope up with a increasing amount of work in an efficient manner .The watermarked video frame is scaled to 0.25, 0.5, 0.6, 0.8.

Cropping: It denotes the removal of the outer parts of an image to enhance framing. Based on the application, it may be performed on a physical photograph, artwork or film footage. It is regarded as a type of noise in the network and detailed investigation is done.

Sharpening: It refers to another type of attack and the image is also tested in sharpened form. It is a type of transformation which helps in bringing out the image details. The edges are sharpened, so that the eye can pick up the image very quickly. Reduced blurring in the image is obtained. Gaussian noise is added to the watermarked image and then removed from it using the median filtering method.

Gaussian noise: It is a kind of statistical noise that has its probability density function equal to that of the normal distribution. It is also known as Gaussian distribution. In many applications, Gaussian noise is mostly utilized as additive white noise to give additive white Gaussian noise.

Median filter is a non linear filtering method and it is used in the reduction of noises for watermarked image samples to improve the quality of the image. The sliding median filter of a pre-specified image window with size W×W centered at image pixels i = (i_1, i_2) progress consistently over the noisy watermarked image g and selects median of the pixels within a specified range of pixels for spatial domain Ω_i^w approximately to have g(i) and noisy image g(i) is replaced by μ. For the set of pixels within a square window WD×WD, centered at i = (i_1, i_2) and defined specified range of pixels for spatial domain Ω_i^w approximately by equation, the median, μ of the pixels in spatial domain Ω_i^w is:

$$u(i) = \mu_i = \text{median}\left\{\frac{g(j)}{j} \in O_i^W\right\} \tag{36}$$

Thus, the output of the median filter is defined as θ which gives lesser error rate results with the entire pixels in the local neighborhood defined by the mask. The output of the median filter at spatial location i can also be specified as:

$$u(i) = \mu_i = \underset{?}{\text{argmin}} \sum_{r \in O^W} |g(r) - \theta|$$

Watermark detection: During watermark detection, the linear correlation described by Eq. 37 is used for detection of the existence of the watermark in the circular regions:

$$\gamma_{1_c} = \frac{1}{S_s} \sum_{VF,F \in s} w.f_s^{'}(VF,F) \tag{37}$$

Where:

γl_c = The linear correlation
s = One of the circular regions
S_s = The area of the region and w is the watermark generated by the same key which is created from SVD and it is used for the watermark embedding process

Watermark detection comprises the following steps:

- Use PN generator for the generation of the same watermark as the one used for watermark embedding
- Location of the RST invariant regions for watermarking using the Non stationary Gaussian scale model
- Calculation of the linear correlation between the watermark and the watermarked data using Eq. 37. The watermark is detected in one circular region when the result is larger than a predefined threshold

The algorithm formulated in this research paper works in the spatial domain and the watermark embedding regions are usually homogeneous because of the selection scheme for the watermarking circular region.

Therefore, the nonlinearity does not produce much improvement in the detector's performance. The following experiments depict the detector's performance. In the tests, 100 different watermarks are embedded into one circular region of the frame image from video and the linear correlation results are computed during the watermark detection. The change of the orientation of reference feature points should be in uniform coherence with the rotation applied to the image. Suppose the initial orientation of a reference feature point is θ_0, after the image is rotated for degree $\theta_0+\theta_1$.

RESULTS AND DISCUSSION

The efficiency of the algorithm can be exhibited using the following five sets of experiments. Four types of attacks are tested: rotation, scaling, cropping, sharpening and Gaussian noise. The algorithm is tested on different video frame images which consist of a variety of portraits, landscapes, people, natural scenes and should be capable of covering most of applications for the image watermarking scheme. The same watermark sequence is embedded into the selected circular regions of several video frame images. The watermark sequence is generated in a random manner under normal distribution. The input video files sample is shown in Fig. 3. The segmented video file sample is shown in Fig. 4.

The Water marked image sample is shown in Fig. 5. The results of the encrypted image matrix and the question image matrix are combined into a single image as shown in Fig. 6. The types of attacks added in the embedded video file sample are shown in Fig. 7 and 8. The extracted image sample is shown in Fig. 9.

Rotation: Under rotation, the algorithm is tested with various rotation angles ranging from 0-300 with a step of 3. The horizontal axis of each sub-figure is indicative of

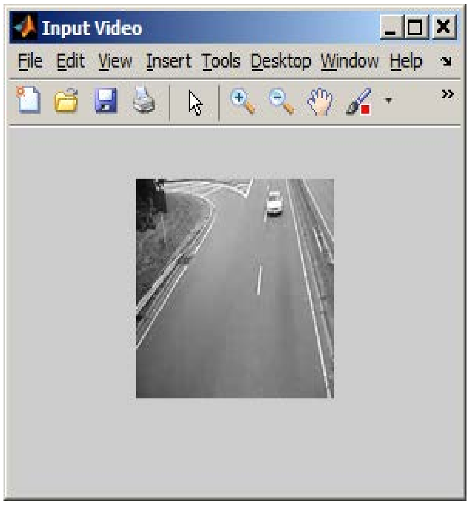


Fig. 3: Video file sample

the rotation angles. The vertical axis conveys the values of linear correlations. Both the false positive probabilities and the false negative probabilities are 0 which means that the watermark can be accurately detected under rotation.

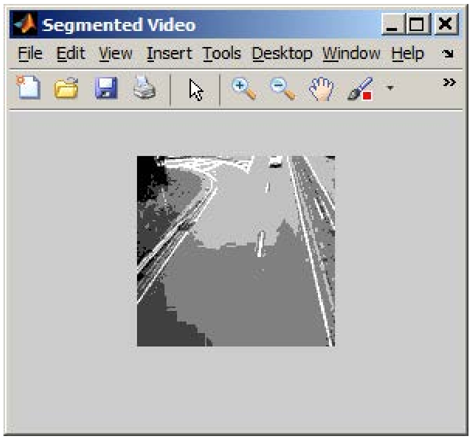
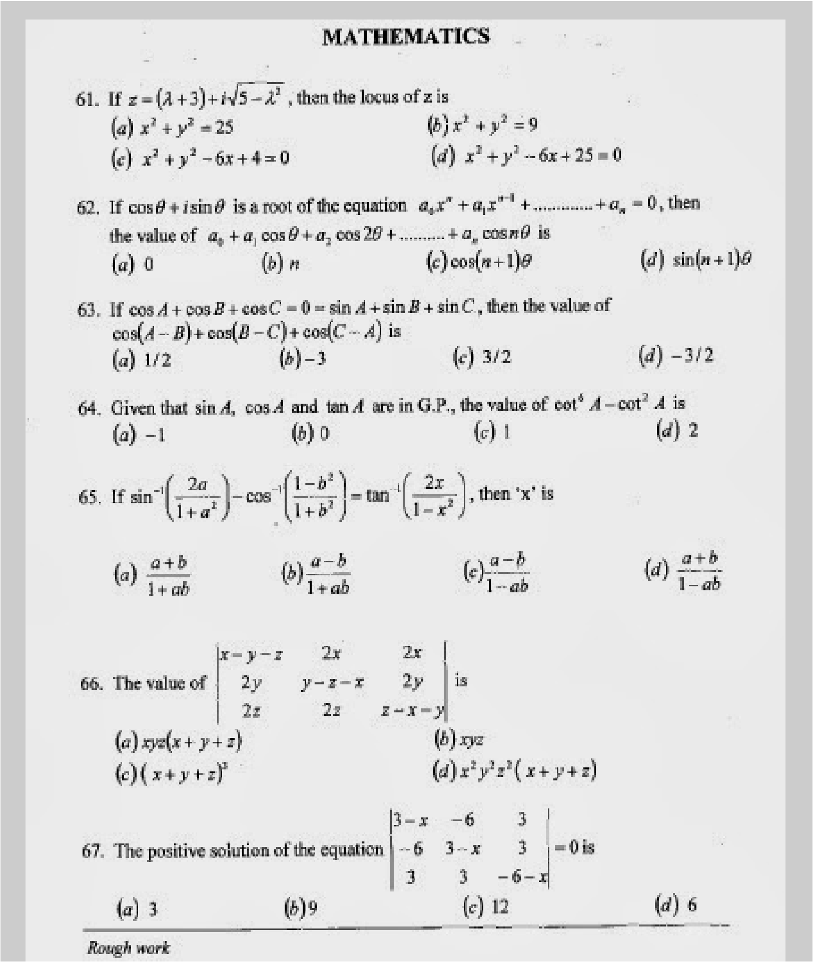


Fig. 4: Segmented video file sample

The horizontal axis of each sub-figure in Fig. 10 displays the rotation angles. The vertical axis indicates the values of linear correlations. The results of the proposed Non-stationary Gaussian distribution with SVD watermarking, Gaussian model (GM), Non Stationary Gaussian Distribution model (NGDM)-SVD and Markov Random Field(MRF)-SVD are compared. It shows that the proposed MRF has high linear correlation than the available methods, since attack resistance analysis is conducted in the proposed work MRF-SVD.

Proposed MRF-SVD algorithm is tested under scaling distortion with scale factor varying from 0.7-1 with a step of 0.1. Results corresponding to the video frames are shown in Fig. 11. The suggested MRF-SVD algorithm performs well against scaling. Also, it is proven that the



MATHEMATICS

61. If $z=(\lambda+3)+i\sqrt{5-\lambda^2}$, then the locus of z is
(a) $x^2+y^2=25$ (b) $x^2+y^2=9$
(c) $x^2+y^2-6x+4=0$ (d) $x^2+y^2-6x+25=0$

62. If $\cos\theta+i\sin\theta$ is a root of the equation $a_0x^n+a_1x^{n-1}+\ldots\ldots\ldots\ldots+a_n=0$, then the value of $a_0+a_1\cos\theta+a_2\cos 2\theta+\ldots\ldots\ldots+a_n\cos n\theta$ is
(a) 0 (b) n (c) $\cos(n+1)\theta$ (d) $\sin(n+1)\theta$

63. If $\cos A+\cos B+\cos C=0=\sin A+\sin B+\sin C$, then the value of $\cos(A-B)+\cos(B-C)+\cos(C-A)$ is
(a) 1/2 (b) -3 (c) 3/2 (d) $-3/2$

64. Given that $\sin A$, $\cos A$ and $\tan A$ are in G.P., the value of $\cot^6 A-\cot^2 A$ is
(a) -1 (b) 0 (c) 1 (d) 2

65. If $\sin^{-1}\left(\frac{2a}{1+a^2}\right)-\cos^{-1}\left(\frac{1-b^2}{1+b^2}\right)=\tan^{-1}\left(\frac{2x}{1-x^2}\right)$, then 'x' is
(a) $\frac{a+b}{1+ab}$ (b) $\frac{a-b}{1+ab}$ (c) $\frac{a-b}{1-ab}$ (d) $\frac{a+b}{1-ab}$

66. The value of $\begin{vmatrix} x-y-z & 2x & 2x \\ 2y & y-z-x & 2y \\ 2z & 2z & z-x-y \end{vmatrix}$ is
(a) $xyz(x+y+z)$ (b) xyz
(c) $(x+y+z)^3$ (d) $x^2y^2z^2(x+y+z)$

67. The positive solution of the equation $\begin{vmatrix} 3-x & -6 & 3 \\ -6 & 3-x & 3 \\ 3 & 3 & -6-x \end{vmatrix}=0$ is
(a) 3 (b) 9 (c) 12 (d) 6

Rough work

Fig. 5: Water mark image

linear correlation values become smaller when the image shrinks or enlarges with a larger ratio. In this technique, MRF-SVD methods also perform well for scaling attack resistant results. The proposed MRF-SVD algorithm is furthermore tested under Gaussian noise pollution. The variance of the noise varies from 0.001-0.1 with a step of 0.001. The results are shown in Fig. 12. The maximum and minimum values for the linear correlation of the watermarked images are 3.1553 and 0.7878.

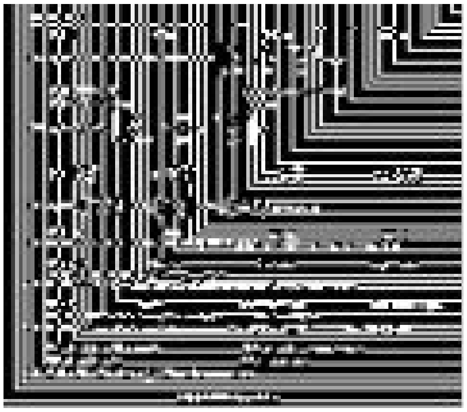


Fig. 6: Encrypted image

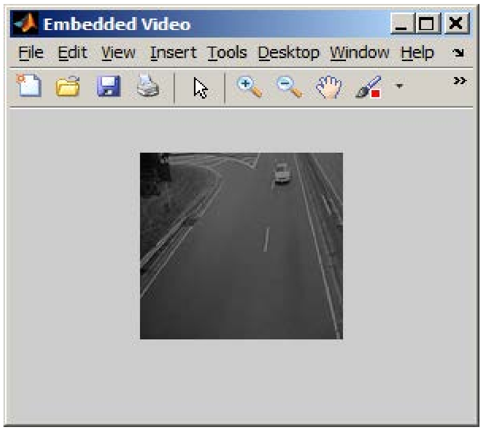


Fig. 7: Embeeded video file sample

Peak Signal to Noise Ratio (PSNR): The ratio between the maximum possible powers to the power of corrupting noise is known as Peak Signal to Noise Ratio. The fidelity of its representation is affected. It can be also described that it is the logarithmic function of peak value of image and mean square error.

$$\mathrm{PSNR} = 10\log_{10}\log_{10}\left(\mathrm{MAX}_i^2 / \mathrm{MSE}\right) \tag{38}$$

Mean square error: Mean Square Error (MSE) of an estimator is the quantification of the difference between an estimator and the true value of the quantity which is being approximated.

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2 \tag{39}$$

The perceptual quality is measured after attacks are added to the watermarked images. The Peak of Signal-to-Noise Ratio (PSNR) is calculated to estimate the quality of the watermarked video frames in comparison

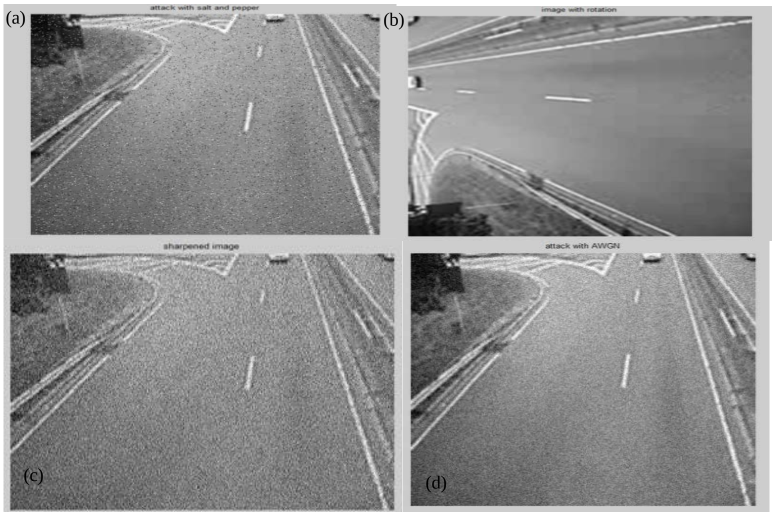
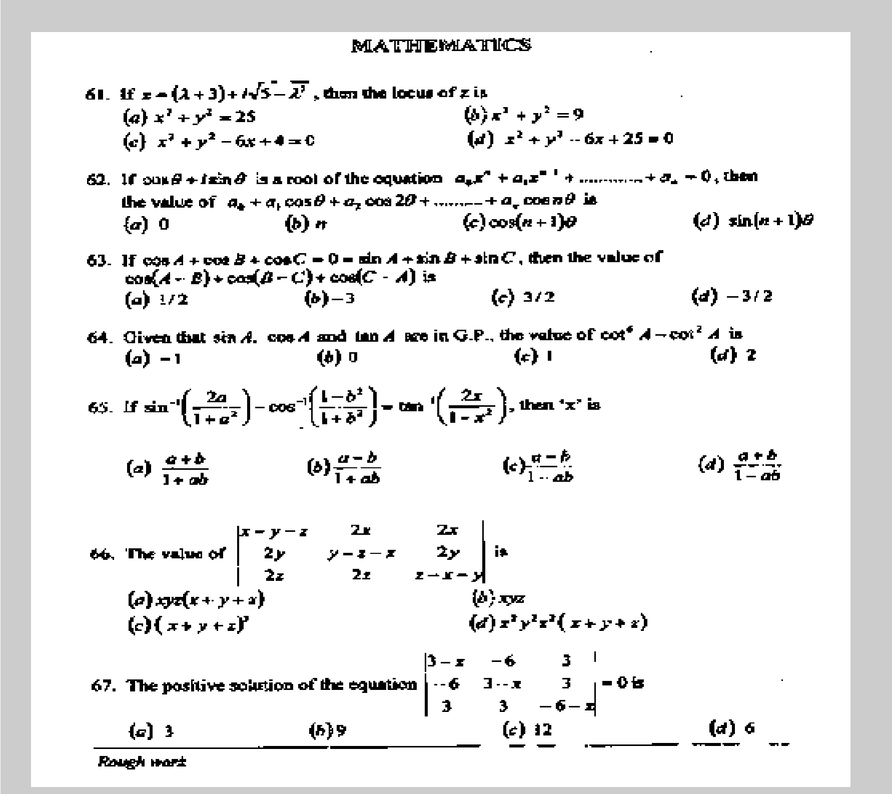


Fig. 8: Attacks added to embedded image samples: a) Salt and pepper noise; b) Rotation; c) Sharpening noise; d) AWGN



MATHEMATICS

61. If $z = (\lambda + 3) + i\sqrt{5 - \lambda^2}$, then the locus of z is
(a) $x^2 + y^2 = 25$ (b) $x^2 + y^2 = 9$
(c) $x^2 + y^2 - 6x + 4 = 0$ (d) $x^2 + y^2 - 6x + 25 = 0$

62. If $\cos\theta + i\sin\theta$ is a root of the equation $a_0x^n + a_1x^{n-1} + \ldots\ldots\ldots + a_n = 0$, then the value of $a_0 + a_1\cos\theta + a_2\cos 2\theta + \ldots\ldots\ldots + a_n\cos n\theta$ is
(a) 0 (b) n (c) $\cos(n+1)\theta$ (d) $\sin(n+1)\theta$

63. If $\cos A + \cos B + \cos C = 0 = \sin A + \sin B + \sin C$, then the value of $\cos(A - B) + \cos(B - C) + \cos(C - A)$ is
(a) $1/2$ (b) -3 (c) $3/2$ (d) $-3/2$

64. Given that $\sin A$, $\cos A$ and $\tan A$ are in G.P., the value of $\cot^6 A - \cot^2 A$ is
(a) -1 (b) 0 (c) 1 (d) 2

65. If $\sin^{-1}\left(\frac{2a}{1+a^2}\right) - \cos^{-1}\left(\frac{1-b^2}{1+b^2}\right) = \tan^{-1}\left(\frac{2x}{1-x^2}\right)$, then 'x' is

(a) $\frac{a+b}{1+ab}$ (b) $\frac{a-b}{1+ab}$ (c) $\frac{a-b}{1-ab}$ (d) $\frac{a+b}{1-ab}$

66. The value of $\begin{vmatrix} x-y-z & 2x & 2x \\ 2y & y-z-x & 2y \\ 2z & 2z & z-x-y \end{vmatrix}$ is
(a) $xyz(x+y+z)$ (b) xyz
(c) $(x+y+z)^3$ (d) $x^2y^2z^2(x+y+z)$

67. The positive solution of the equation $\begin{vmatrix} 3-x & -6 & 3 \\ -6 & 3-x & 3 \\ 3 & 3 & -6-x \end{vmatrix} = 0$ is
(a) 3 (b) 9 (c) 12 (d) 6

Rough work

Fig. 9: Extracted image samples

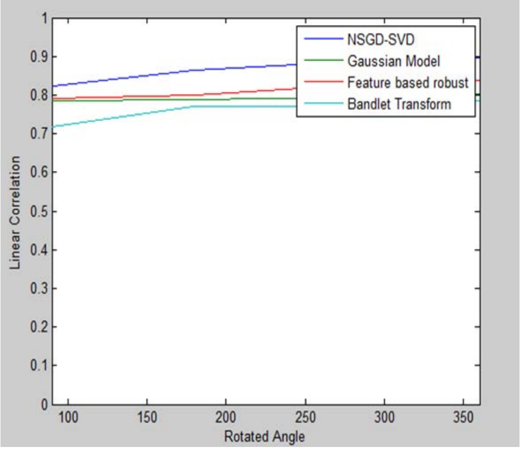


Fig. 10: Rotated angles vs. linear correlation

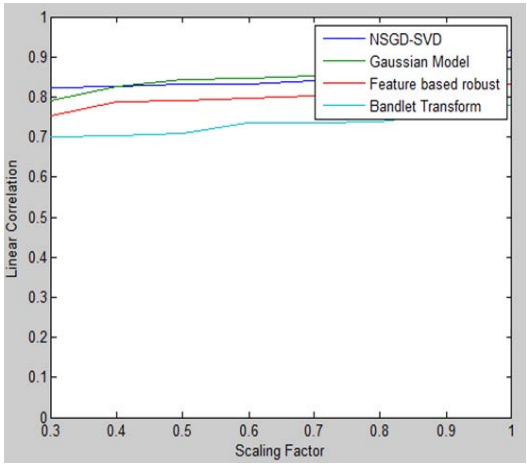


Fig. 11: Scale factor vs. linear correlation

with the original ones. The performance of the proposed MRF-SVD scheme is compared with the existing watermarking GM and NGDM-SVD. The PSNR results of the proposed MRF-SVD schema is higher after the attacks such as scaling, rotation, sharpening, Cropping and filtering when compared to existing watermarking methods is shown in Fig. 13.

The comparison of the performance of the MRF-SVD scheme is done with the already available watermarking GM and NGDM-SVD schemes for MSE comparison. In the scientific work, MRF-SVD MSE is computed between the watermarked images and watermarked with attacks

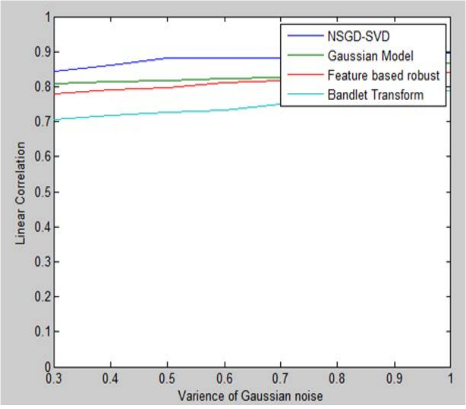


Fig. 12: Experimental results against gaussian noise pollution

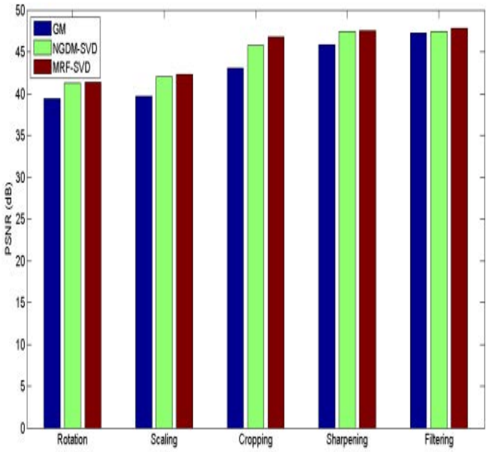


Fig. 13: Experimental results of PSNR comparison against attacks

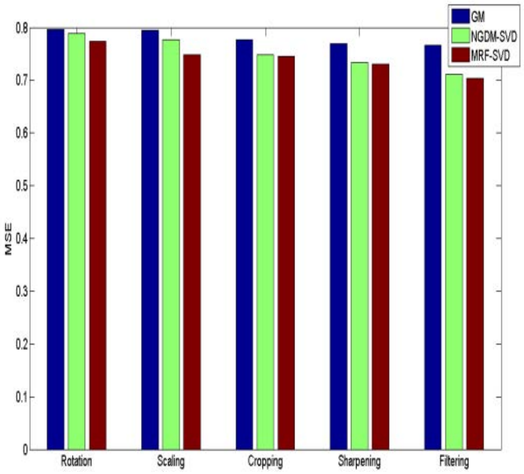


Fig. 14: Experimental results of MSE comparison against attacks

detected image which reveals that the MSE results of the proposed MRF0-SVD have reduced MSE error rate for all types of attacks as shown in Fig. 14.

CONCLUSION

In this research, a relatively new video watermarking technique to model video frames using the Markov Rrandom Field in spatial domain is proposed. The video frames are first segmented using K-Dependence Bayesian (KDB) into several homogeneous areas. Each region is then denoted utilizing Markov Random Field (MRF). The MRF model is used to locate the salient feature points which can be used as the reference points and are useful for defining the circular regions for the watermark embedding or detection procedures. After the salient features are selected it is protected using the SVD method. Frame encryption techniques scramble the feature point's pixels of the frames and reduce the correlation among the pixels, so that lower correlation among the pixels and the encrypted frame is obtained. Hence, the features within each embedding or detection region are consistent. In embedding stage the text files are embedded in the encrypted frame matrix. It gives better guidance for adaptive adjustment of the watermark embedding strength utilizing NVF. Attack resistance analysis is conducted on the watermarked video frame. In this stage, removal of Gaussian noise is performed using the median filtering techniques and sharpening is also done to find attacks in the video embedded frame. The results obtained from experiments depict that the studied MRF-SVD algorithm is a good performer against rotation, scaling, cropping, sharpening and Gaussian noise removal computed using PSNR and MSE. The capability of the watermarking algorithm can be enhanced if some other perceptual models instead of NVF can be brought into place. In addition, contrast sensitive function and texture sensitive function can be used here. The spread spectrum is useful for watermark embedding and gives good performance of robustness. Other coding techniques and modulation can also be put in place, particularly after the image is segmented into different regions which can be dealt as parallel transmission channels.

REFERENCES

Al-Taweel, S.A. and P. Suma, 2009. Robust video watermarking based on 3D-DWT domain. Proceeding of the IEEE, Conference on TENCON Region 10, January 23-26, 2009, IEEE, Singapore, ISBN: 978-1-4244-4546-2, pp: 1-6.

Bhatnagar, G. and B. Raman, 2012. Wavelet packet transform-based robust video watermarking technique. Sadhana, 37: 371-388.

Coria, L., P. Nasiopoulos, R. Ward and M. Pickering, 2007. An access control video watermarking method that is robust to geometric distortions. J. Inform. Assurance Secur., 2: 266-274.

Elbasi, E., 2007. Robust Video Watermarking Scheme. ProQuest, Ann Arbor, Michigan, USA., Pages: 193.

Fouda, Y.M., 2015. A robust template matching algorithm based on reducing dimensions. J. Signal Inf. Process., 6: 109-122.

Jayamalar, T. and V. Radha, 2010. Survey on digital video watermarking techniques and attacks on watermarks. Intl. J. Eng. Sci. Technol., 2: 6963-6967.

Lowe, D.G., 2004. Distinctive image features from scale-invariant keypoints. Intl. J. Comput. Vis., 60: 91-110.

Mirza, H.H., H.D. Thai, Y. Nagata and Z. Nakao, 2007. Digital video watermarking based on principal component analysis. Proceeding of the 2nd International IEEE Conference on Innovative Computing, Information and Control, September 5-7, 2007, IEEE, Kumamoto, Japan, ISBN: 0-7695-2882-1, pp: 290-290.

Mostafa, S.A.K., A.S. Tolb, F.M. Abdelkader and H.M. Elhindy, 2009. Video watermarking scheme based on principal component analysis and wavelet transform. Int. J. Comput. Sci. Network Security, 9: 45-52.

Park, H., S.H. Lee and Y.S. Moon, 2006. Adaptive Video Watermarking Utilizing Video Characteristics in 3D-DCT Domain. In: Digital Watermarking. Shi, Y.Q. and B. Jeon (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-540-48825-5, pp: 397.

Rubio, A. and J.A. Gamez, 2011. Flexible learning of k-dependence Bayesian network classifiers. Proceedings of the 13th Annual ACM Conference on Genetic and Evolutionary Computation, July 12-16, 2011, ACM, New York, USA., ISBN: 978-1-4503-0557-0, pp: 1219-1226.

Sajasi, S. and A.M.E. Moghadam, 2013. A high quality image hiding scheme based upon noise visibility function and an optimal chaotic based encryption method. Proceeding of the 5th RoboCup Iran Open International Symposium and 3rd Joint IEEE Conference on AI & Robotics and RIOS, April 8, 2013, IEEE, Tehran, Iran, pp: 1-7.

Seo, J.S. and C.D. Yoo, 2006. Image watermarking based on invariant regions of scale-space representation. IEEE Trans. Signal Process., 54: 1537-1549.

Wang, L., H. Ling, F. Zou and Z. Lu, 2011. Real-time compressed-domain video watermarking resistance to geometric distortions. IEEE. MultiMedia, 19: 70-79.

Yuan, X.C. and C.M. Pun, 2013. Feature based video watermarking resistant to geometric distortions. Proceeding of the 12th International IEEE Conference on Trust, Security and Privacy in Computing and Communications, July 16-18, 2013, IEEE, Melbourne, Victoria, Australia, pp: 763-767.

Zheng, D., S. Wang and J. Zhao, 2009. RST invariant image watermarking algorithm with mathematical modeling and analysis of the watermarking processes. Image Process. IEEE. Trans., 18: 1055-1068.

Zheng, D., Y. Liu and J. Zhao, 2007. A survey of RST invariant image watermarking algorithms. ACM Comput. Surv., Vol. 39. 10.1145/1242471.1242473.