Research Journal of Applied Sciences, Engineering and Technology 11(6): 603-609, 2015
DOI: 10.19026/rjaset.11.2019
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: February 13, 2015 Accepted: March 20, 2015 Published: October 25, 2015

Research Article

Design and Analysis of a High Secure Video Encryption Algorithm with Integrated Compression and Denoising Block

T. Vino and E. Logashanmugam
Sathyabama University, Chennai, India

Abstract: This study investigates the design of High Secure Video Encryption with self-integrated compression and denoising block. Depending on the magnitude of the wavelet co-efficient and noise variance for each co-efficient in the hybrid compressor is estimated based on the sub band using the Maximum Likelihood Estimator and Maximum a Posterior (MAP) estimator. The Adaptive threshold is applied to each sub band co-efficient except the approximation sub band of the wavelet. The resultant will yield a superior quality by removing the noise in the video signals obtained during acquisition or transmission of video. The need of an efficient compression Block in the Video encryption is because the original video consumes more bit rate for transmission and storage. The Proposed algorithm is tested with test video considering the PSNR, MSE for evaluation.

Keywords: Chaotic neural network, denoising video signal, video encryption

INTRODUCTION

Video Encryption is a key research area for researchers due to the increase in Amount of Information Transmitted through Video signals in the unsecured channel. The attack on the information sent through an unsecured channel has greatly found an increase due to many reasons. The Responsibility of protecting Information sent through an Unsecured Channel relies with the Sender. Apart from the data hackers, the attack may also happen in many ways. One of the common way is the attack caused due to the noise in the environment. So the Algorithm that is applied on the Information at the sender end before transmitting in the unsecured channel should be able to protect the information from these attacks. In our previous paper, we had provided an efficient solution using Chaotic Neural Network for protecting the Video Signals from the data hackers as described in Vino and Logashanmugam (2014). In this study, we delve into the topic of denoising, extending the work presented in Vino and Logashanmugam (2014). Our previous paper concentrates mainly on Video Encryption using Chaotic Neural Network and we had provided an external Compression block in the pre-processing step to reduce the amount of information transmitted through the channel. As an extension, in this study we had proposed an efficient hybrid algorithm for video signals that will denoise, compress and encrypt the video signal using the wavelet and Chaotic Neural Network.

Wavelet Shrinkage is a method of removing the noise from the image by shrinking the empirical Wavelet co-efficeints in the wavelet domain. This de-noising is non-linear by nature. Thresholding is the common shrinkage approach that sets the wavelet co-efficient with small magnitude to Zeros and the rest is maintained with ones. In the literature, Donoho and Johnston (1994, 1995) suggested to use the global threshold uniformly throughout the entire wavelet decomposition tree for efficient performance. Although it is simple by nature, the amount of noise removed is not satisfactory. Adapting a Threshold for removing the noise is the efficient process and also the amount of noise removed is comparatively more than the Global Uniform Threshold (Donoho, 1995; Donoho, 1993; Zhong and Cherkassy, 2000; Donoho and Johnstone, 1995; Chang *et al*., 2000a). Chang *et al*. (2000b) gave a method for spatially adaptive wavelet thresholding with context modeling for image denoising. Chang *et al*. (1997) introduced a method that bridges the operation of compression to wavelet thresholding as a denoising. Kalavathy and Suresh (2011) made analysis of image denoising using Wavelet coefficient and introduced adaptive subband Threshold Technique. Alirezaei and Yaghbi (2010) introduced an efficient video encryption based on a image key for hyper-chaos system. Asim and Jeoti (2007) gave image encryption based on AES and a novel chaotic encryption scheme. Behnia *et al*. (2012) introduced a method based on quantum chaotic map and FSM transforms. In this study, we use a Maximum Likelihood Estimator for estimating the noise variance for each wavelet co-efficient depending on the sub-band for each video frame. An adaptive threshold is applied to each sub band co-efficient except the approximation sub band of the wavelet. A

Corresponding Author: T. Vino, Sathyabama University, Chennai, India
This work is licensed under a Creative Commons Attribution 4.0 International License (URL: http://creativecommons.org/licenses/by/4.0/).

multiplying factor is included in the optimum threshold formula that makes the threshold value dependent on the decomposition level. The soft threshold is applied to each noisy co-efficient. The reconstructed video frame will be superior in quality with the noise removal. The aim of the work is to design a high Secure Video Encryption with inbuilt compression and noise elimination block.

MATERIALS AND METHODS

Discrete wavelet transform: The simplest of Discrete Wavelet Transform is Haar-DWT where the low frequency wavelet coefficients are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. For 2D-images, applying DWT will result in the separation of four different bands. LL is the lower resolution approximation of the image. HL is the horizontal, LH is the vertical, HH is the diagonal component. The Low frequency band consists of smooth part of the image and the High frequency sub band will contain the edge and texture details.

Estimation of noise variance in the video frame: For each video frame the wavelet transform is applied and the below steps are used for evaluating the Noise variance for each wavelet co-efficient.

Step 1: Using the accurate median estimator, the noise variance σ_V^2 can be accurately estimated from the first decomposition level diagonal sub band HH_1:

$$\sigma_V^2 = \left(\frac{median|y(V)|}{0.6745}\right)^2 \quad (1)$$

where, $y(V)$ represents the coefficients HH_1 sub band.

Step 2: The coarse sub bands are not processed because the coarse sub band has very high SNR. These coefficients are considered reliable.

Step 3: For each of the three sub bands (horizontal, vertical and diagonal orientations) coefficients within the sub band are modeled as identically independently distributed with zero mean and variance $\sigma^2_{x,j}$ (where j indicates the Sub band). The variance estimate is computed from the noisy coefficients in sub band j as:

$$\sigma^2_{x,j} = max\ \{0, var\{\bar{y}_i, i \in subbandj\} - \sigma_V^2\} \quad (2)$$

Using MAP, estimation of $\bar{x}$ is obtained by applying a soft threshold λ as given in Eq. (3) to each noisy coefficient:

$$\lambda = \sqrt{2}\sigma^2_V / \sigma^2_{x,j}, j \in subband \quad (3)$$

Step 4: In each of the other high sub bands, coefficients are assigned either significant or insignificant classes depending on the magnitude of their estimated parent relative to the significance threshold T, where T is given by:

$$T = \sigma\sqrt{2log\ N^2} \quad (4)$$

- Coefficients in significant class are modeled as 2d Laplacian with zero mean and their variance $\sigma^2_{x,insig}$ is estimated from the noisy coefficients as mentioned in step 3. Again the MAP estimator is a simple soft thresholding scheme where its threshold value is adjusted to the signal variance.
- Coefficients in insignificant class which has small magnitude representing smooth areas, $\sigma^2_{x,insig}$ is estimated using ML estimator in order to have an estimate for a local neighborhood σ^2_x where variance is assumed to be constant. Thus the estimate of the class coefficient variance is given by:

$$\sigma^2_{x,insig} = \frac{1}{M}\left(\sum_{V=1}^{M} y^2\,(V) - \sigma_V^2\right) \quad (5)$$

where, M represents the number of wavelet coefficients residing in local neighborhood N. Considering the coefficients belonging to a insignificant class inside the window are used by excluding the one which belong to significant class, the Maximum a Posterior (MAP) estimator is given by:

$$\bar{x} = \frac{\sigma^2_{x,insig}}{\sigma^2_{x,insig} + \sigma_V^2}\,\bar{y}_i \quad (6)$$

Hence the coefficient of estimates corresponding to the high sub band are obtained by repeating the above steps from parent to child sub band, starting from the coarse scale and terminating in the highest sub band.

Threshold selection: Threshold plays a major part in denoising technique. The Small the threshold may not perform well similarly the large threshold may lead to loss of information. Soft thresholding may provide better performance but it leads to distortion of information (Chang, 2000). A common approach is to obtain the sample variance σ^2 of the coefficient of a band and set the threshold to any multiple of the σ for that band (Kalavathy and Suresh, 2011). The soft threshold is represented by the equation:

$$d^{soft}_{ik} = \text{sign}\,(d_{ik})(|d_{ik}| - \lambda^*) \text{ if } d_{ik} > \lambda^* \quad (7)$$
$$= 0 \text{ if } d_{ik} \le \lambda^*$$

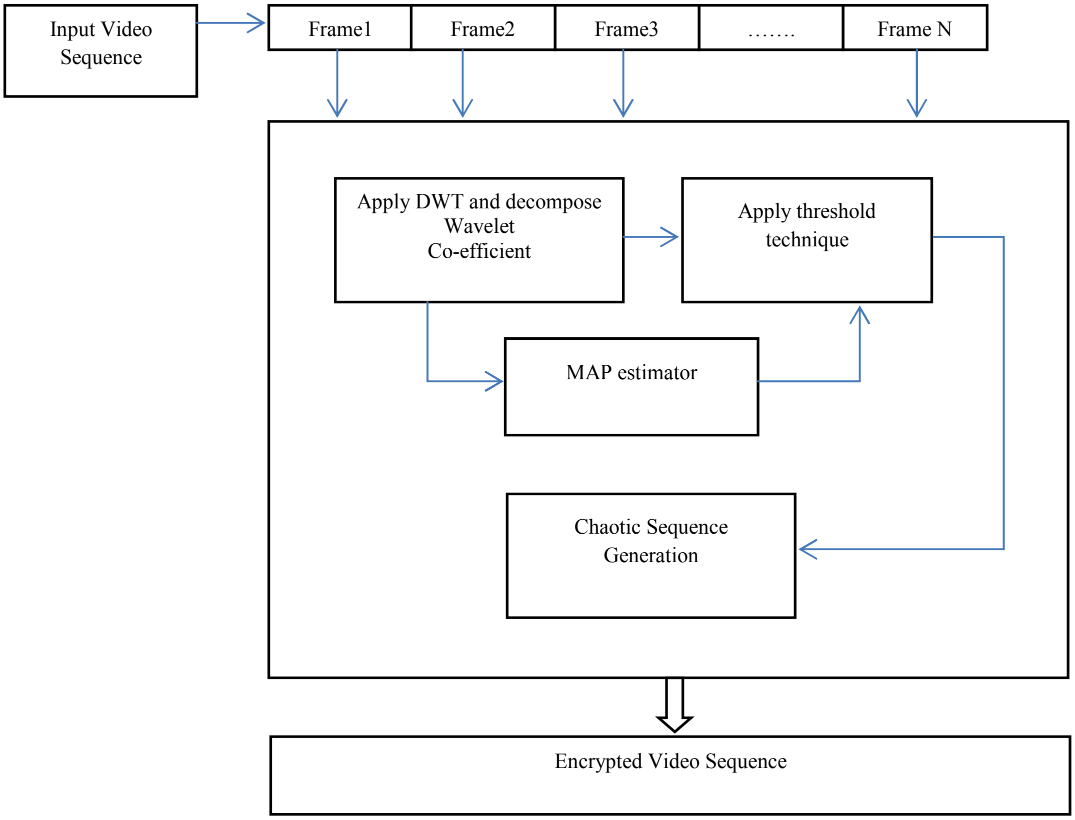


Fig. 1: Block diagram of chaotic encryption

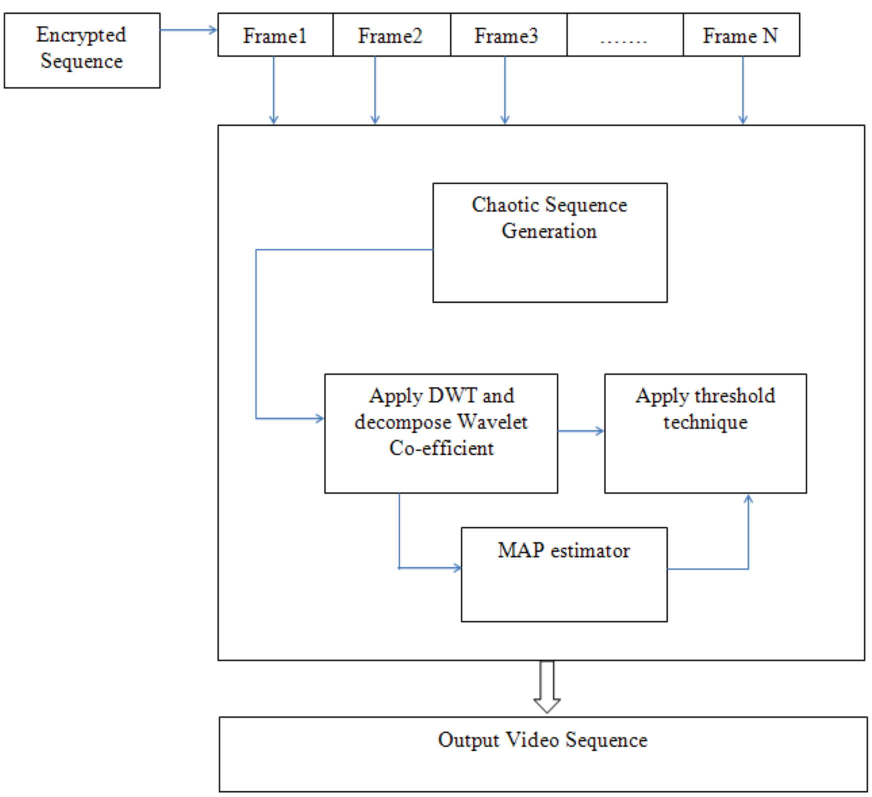


Fig. 2: Block diagram of chaotic decryption

To preserve the quality of the video frame the multiplying factor α is multiplied with the threshold (4) as provided in (Vino and Logashanmugam, 2014):

$$\alpha = 2^{L-K}\sqrt{\log M} \tag{8}$$

The new adaptive threshold will be represented by the below equation:

$$\lambda^* = \alpha\,\lambda \tag{9}$$

Proposed algorithm: The Proposed algorithm is better explained using the block diagram Fig. 1 and 2. The Proposed Video Encryption algorithm is a highly efficient algorithm in terms of Security and Quality.

Algorithm:
The algorithm of the proposed algorithm is as follows.
Input: Video frame
Output: Encrypted frame

1. Read the video and convert into frames.
2. Perform Multi scale decomposition of the video corrupted by Gaussian noise using wavelet transform.
3. Estimate the noise variance *V* σ using Eq. (1) for each scale and compute the scale parameter.
4. For each of the three sub bands variance estimate is computed from the noisy coefficient in sub band j using Eq. (2)
5. In each of the other high sub bands the estimates of the class coefficient variance are estimated using Eq. (2) and (5).
6. Calculate threshold value using optimum value threshold formula as given in Eq. (9) after finding the multiplying factor σ for each sub band using the relation given in (8) After computing threshold for each sub band except the low pass or approximation sub band, apply soft thresholding to each wavelet coefficient using threshold given in Eq. (7), by substituting the threshold value obtained in Step 6.
7. Step 6 of frames is converted into a 1D matrix.
8. Calculate the length of the 1D matrix and divide the 1D matrix into subsequences of 8 bytes.
9. Set the Parameters, μ and the initial point x (0)
10. The chaotic sequence x (1), x (2), x (3)…. X (M) is evolved using the formula:

    X (n+1) = μx (n) (1-x (n))

11. Create b (0),b (1)…b (8M-1) from x (1), x (2)….x (M)
    by the generating scheme that b(8m-8)b(8m-7)…b(8m-1)… is the binary representation of x(m) for m = 1, 2,…M.
12. For n = 0 to (M-1)
    For i = 0 to 7
    j = {0, 1, 2, 3, 4, 5, 6, 7}
    Wji =1 if j = i and b (8n+i) = 0
    -1 if j = i and b (8n+i) = 1
    0 if j≠i
    Θ_i = - ½ if b (8n+i) = 0
    ½ if b (8n+i) =
    End
    For i = 0 to 7, d_i is calculated using:
    di = f ($\sum_{i=0}^{i=7} W_{ij}\ d_i + \theta_i$)

    where, f(x) is 1 if x> = 0
    End:
    g(n) = $\sum_{i=0}^{i=7} d_i\ 2^i$
    End
    Thus the encrypted signal (*g*) is obtained.
13. Invert the multiple decomposition to construct the encrypted video frame.

RESULTS AND DISCUSSION

Quality evaluation for proposed algorithm and results: To facilitate the efficiency of the proposed algorithm, the Statistical Measure of the Objective Quality Assessment has been performed for each frame in the video signal. A brief overview of the Objective VQA that is applied for the algorithm is provided below.

Objective VQA: Objective VQA is broadly classified into two different categories. Statistical measures and Human Visual System (HVS).

Statistical measures: Based on Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) the Quantitative performance of the proposed algorithm is evaluated and the equation is given below:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{10}$$

$$\text{MSE} = \frac{\sum_i \sum_j (r_{ij} - x_{ij})2}{M \times N} \tag{11}$$

where, *r* refers to Original video frame, *x* denotes restored frame, M×N is the size of Processed frame.

Human visual system: Several IQA metrics has been developed like Structural Similarity Index Model (SSIM), Visual Signal to Noise Ratio (VSNR). These HVS shows the better correlation with the quality of the video.

Simulation results: The experiment was performed on a core i3 with 2.77 GHz, 3 GB RAM and full cache. To ensure the deepness of the algorithm on each frame, the coast guard video is taken for testing and this video is converted into frames and the algorithm is applied on

Table 1: Comparison of PSNR of different wavelet shrinkage for different noise level corrupted by Gaussian noise

PSNR (DB) Frame	Noise level	Baye's shrink	Normal shrink	Modified Baye's shrink	Adaptive threshold
1	10	48.5715	48.9663	48.6871	49.6713
	20	41.3762	41.6781	41.4682	42.2258
	30	37.3929	37.6487	37.4729	38.1145
2	10	48.5587	48.954	48.6779	49.6621
	20	41.3663	41.6706	41.4596	42.2184
	30	37.3874	37.6448	37.4684	38.1111
3	10	48.5524	48.9506	48.6690	49.6607
	20	41.3654	41.6686	41.4590	42.2174
	30	37.3804	37.6376	37.4611	38.1055
4	10	48.5550	48.9534	48.6708	49.6643
	20	41.3637	41.6639	41.4554	42.2156
	30	37.3807	37.6369	37.4618	38.1068
5	10	48.5474	48.9418	48.6627	49.6511
	20	41.3501	41.6523	41.4413	42.2023
	30	37.3694	37.6281	37.4503	38.0953

Table 2: Comparison of MSE of different wavelet shrinkage for different noise level corrupted by Gaussian noise

MSE (DB) Frame	Noise level	Baye's Shrink	Normal shrink	Modified Baye's Shrink	Adaptive threshold
1	10	0.0077	0.0074	0.0076	0.0069
	20	0.0159	0.0154	0.0158	0.0146
	30	0.0237	0.0231	0.0235	0.0221
2	10	0.0077	0.0074	0.0076	0.0069
	20	0.0159	0.0154	0.0158	0.0146
	30	0.0237	0.0231	0.0235	0.0221
3	10	0.0077	0.0074	0.0076	0.0069
	20	0.0159	0.0155	0.0158	0.0146
	30	0.0238	0.0231	0.0236	0.0022
4	10	0.0077	0.0074	0.0076	0.0069
	20	0.0159	0.0155	0.0158	0.0146
	30	0.0238	0.0231	0.0236	0.0221
5	10	0.0077	0.0074	0.0077	0.0069
	20	0.0160	0.0155	0.0158	0.0146
	30	0.0238	0.0232	0.0236	0.0221

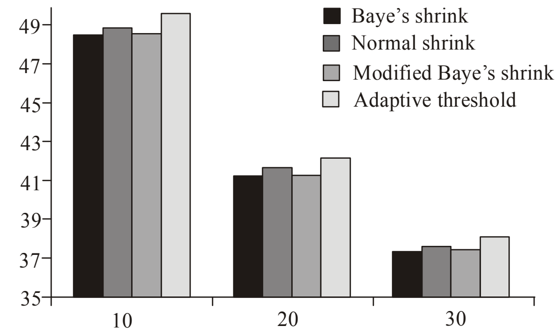


Fig. 3: Comparison of PSNR values for different wavelet shrinkage for different noise level corrupted by Gaussian noise for first frame

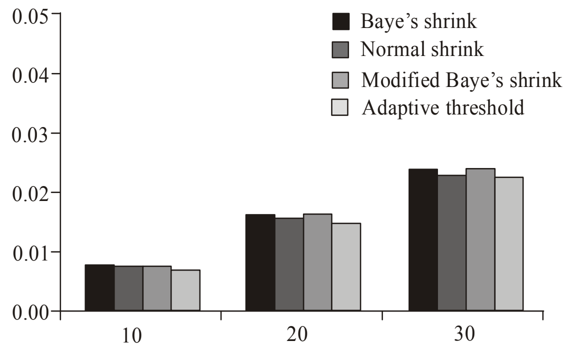


Fig. 4: Comparison of MSE values for different wavelet shrinkage for different noise level corrupted by Gaussian noise for first frame

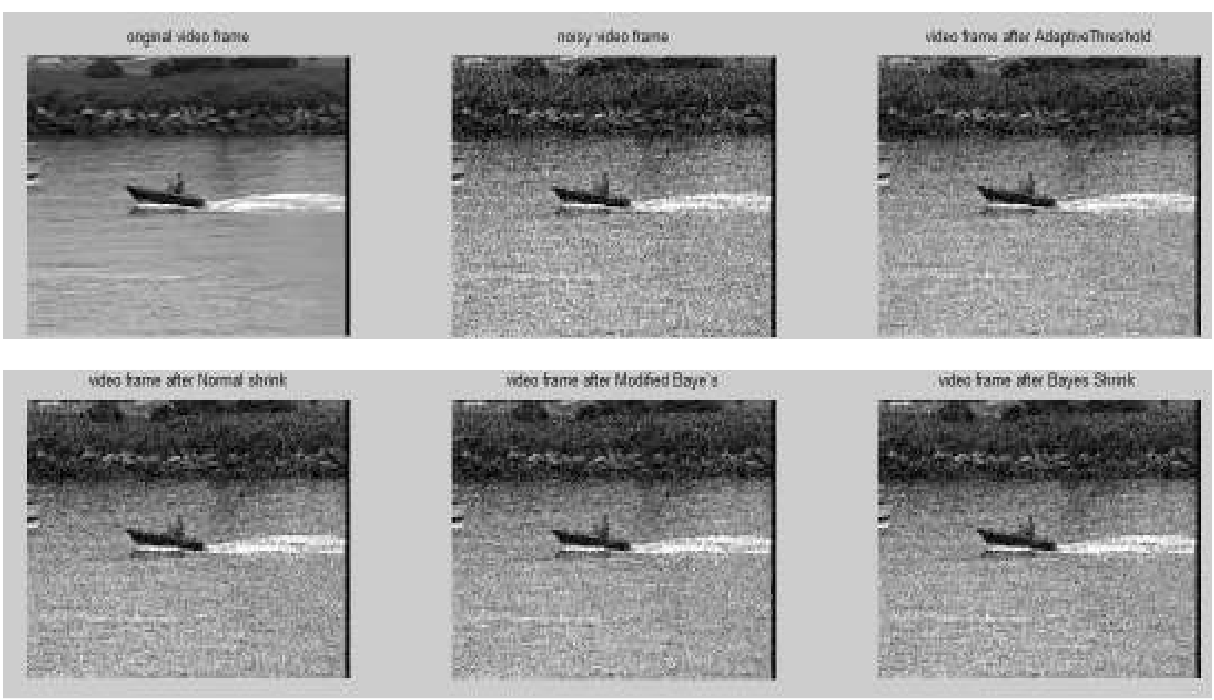


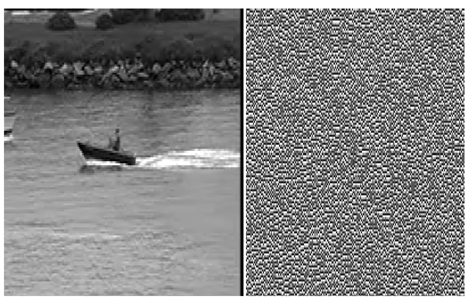
Fig. 5: Comparison of different wavelet shrinkage for noise level 10% corrupted by Gaussian noise for the first frame

Table 3: Performance of the proposed algorithm with adaptive threshold for the entire video sequence

Factor	Value
Number of frames	300
Compression ratio	62.9340
MSE	2.3025e+04
PSNR	4.5427
Processing time	19.8028

Table 4: Comparison of statistical measures of the Encrypted video using the proposed algorithm for different noise level

Noise level	PSNR	MSE
10	4.5413	2.3033e+04
20	4.5424	2.3016e+04
30	4.5596	2.2936e+04
40	4.5992	2.2728e+04
50	4.6653	2.2384e+04



(a) (b)

Fig. 6: (a): Input video 1st frame; (b): proposed encrypted output

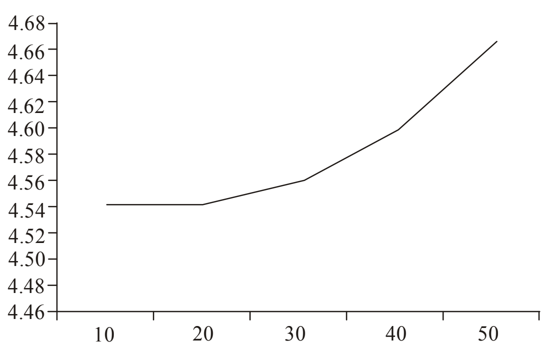


Fig. 7: PSNR of the proposed algorithm for the entire video frame at different noise levels

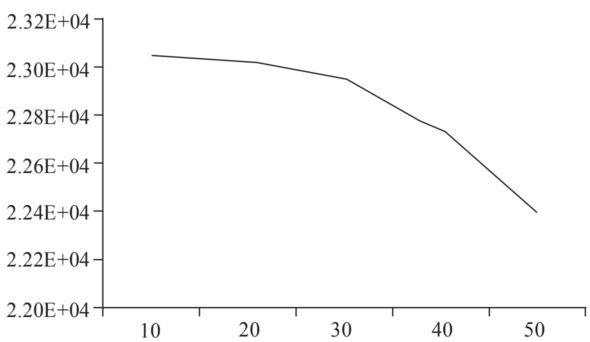


Fig. 8: MSE of the proposed algorithm for the entire video frame at different noise levels

each frame for various noise densities and its statistical measure is studied for first 5 frames. The same is tabulated in this section for reference.

Table 1 and 2 shows the performance comparison of wavelet based denoising technique performed on video frame at different noise levels. From these tables the adaptive thresholding technique used in the proposed algorithm performs better than the other denoising techniques. Figure 3 and 4 shows the graphical representation of the performance comparison of wavelet based denoising technique performed on the video frames at different noise levels.

Figure 5 shows the qualitative analysis for Human visual measure on various wavelet based denoising techniques performed on the First video frame with 10% noise density From Fig. 5. The Adaptive thresholding provides a better result compared to others.

Table 3 shows the performance of the proposed algorithm with adaptive threshold for the entire video sequence. Table 4 discusses the performance of the proposed algorithm for the entire video frame at different noise levels that is corrupted by the Gaussian noise. Figure 6 shows the original frame1 and the encrypted frame 1 of the coast guard video.

Figure 7 and 8 discusses the performance of the proposed algorithm for the entire video frame at different noise levels that is corrupted by the Gaussian noise.

CONCLUSION

In this study an efficient video encryption algorithm that will compress, denoise and encrypt the video signal is presented. This algorithm uses the adaptive threshold and chaotic Neural Network, which is highly secure in nature. The proposed algorithm is tested with different noise levels and to ensure the deepness of the algorithm on each frame, the performance metrics is studied for each frame. The qualitative and quantitative analysis was performed on the proposed algorithm. The proposed algorithm shows the better performance in terms of quality of the video frames and also shows the better compression ratio leading to the significant reduction in memory space.

REFERENCES

Alirezaei, V. and M. Yaghbi, 2010. Efficient video encryption by image key based on hyper-chaos system. Proceeding of the International Conference on Multimedia Communications (Mediacom). Hong Kong, pp: 141-144.

Asim, M. and V. Jeoti, 2007. On image encryption: Comparison between AES and a novel chaotic encryption scheme. Proceeding of the 7th International Conference on Signal Processing, Communications and Networking. IEEE explore Press, Chennai, India, pp: 65-69.

Behnia, S., P. Ayubi and W. Soltanpoor, 2012. Image encryption based on quantum chaotic map and FSM transforms. Proceeding of the 25th International Telecommunications Network Strategy and Planning Symposium. IEEE Press, Rome, Oct. 15-18, pp: 1-6.

Chang, S.G., B. Yu and M. Vetterli, 1997. Bridging compression to wavelet thresholding as a denoising method. Proceeding of the Conference on Information Sciences Systems. Baltimore, MD, pp: 568-573.

Chang, S.G., Y. Bin and M. Vetterli, 2000a. Adaptive wavelet thresholding for image denoising and compression. IEEE T. Image Process., 9(9): 1532-1546.

Chang, S.G., Y. Bin and M. Vetterli, 2000b. Spatially adaptive wavelet thresholding with context modeling for image denoising. IEEE. T. Image Process., 9(9): 1522-1531.

Donoho, D.L., 1993. Nonlinear wavelet methods for recovery of signals, densities and spectra from indirect and noisy data. Proceeding of Symposia in Applied Mathematics, 04: 173-205.

Donoho, D.L., 1995. De-noising by soft-thresholding. IEEE T. Inform. Theory, 41: 613-627.

Donoho, D.L. and I.M. Johnstone, 1994. Ideal spatial adaptation by wavelet shrinkage. Biometrika, 81(3): 1-30.

Donoho, D.L. and I.M. Johnstone, 1995. Adaptive to unknown smoothness via wavelet shrinkage. J. Am. Stat. Assoc., 90(90): 1200-1224.

Kalavathy, S. and R.M. Suresh, 2011. Analysis of image denoising using wavelet coefficeint and adaptive subband threshold technique. IJCSI Int. J. Comput. Sci., 8(1): 166-172.

Vino, T. and E. Logashanmugam, 2014. High capacity and high secure video encryption based on hopfield chaotic neural network. Int. J. Appl. Eng. Res., 9(22): 13113-13135.

Zhong, S. and V. Cherkassy, 2000. Image denoising using wavelet thresholding and model selection. Proceedings on IEEE International Conference on Image Processing, 3: 262-265.