A Newly Proposed Light-Weight Technique to Secure Videos

Ronak Dak[1], Dharm Singh[2], Naveen Choudhary[3]

[1]M. Tech, Department of Computer Science, College of Technology and Engineering
MPUAT, Udaipur, Rajasthan, India

[2]Assistant Professor, Department of Computer Science, College of Technology and Engineering
MPUAT, Udaipur, Rajasthan, India

[3]Professor & Head, Department of Computer Science, College of Technology and Engineering
MPUAT, Udaipur, Rajasthan, India

Abstract: ***In this growing digital world, everything is on air and a lot of multimedia data flows online every second. Day by day more and more multimedia technologies are being introduced and videos are the emerging multimedia content to be taken care of. There are several fields like military, medical and commercial susceptible information that need to be secured or may only be shown partially to the users. Over the last few years numerous encryption algorithms are introduced to secure and protect the video during transmission. Along with that many efficient multimedia encryption schemes are introduced and real world is using those techniques. In this paper, a new technique is proposed to secure the transmission of the video over wireless networks. This technique includes the functionality of three algorithms and introducing a more efficient technique to encrypt the video sequences. This technique is to encrypt the individual frame and using this technique over all video frame sequences to encrypt the video and this will multiply the security effects of the single frame over the full video sequence.***

General Terms: Pattern Recognition, SCAN Based Patterns, Security, Algorithms et. al.

Keywords: SCAN, DES, Encryption, Entropy, NPCR, UACI

1. Introduction

Information is most important thing in today's digital world. Secure Transmission of this information is great concern. There are many issues of security such as intrusion of people privacy, eavesdropping, hacker-attacks. In-spite of all these security concerns we need to transfer information in a secured manner. Today, the combination of digital media and digital devices such as, combination of digital TV with digital video plays a very important role in today's digital world. Now, the next greatest concern is to transfer videos or digital content from digital libraries to the digital devices over wireless networks for e.g. Video on Demand. Since, the videos are of large size, less compression ratio, less or no encryption. So, before sending these videos, they need to be compressed and encrypted. Videos which are transmitted for the entertainment purpose need not to be secured but, video content such as military information or private business content requires to be secured at an efficient level.

To address all the above concerns, video encryption technology came into limelight. There are various methods which enable us to encrypt parts of video frames to secure them but, problem with all these techniques is that all of them focus on complete video data, which results in much computation overhead and resource requirement. So, here we are proposing an efficient video encryption technique which will be light weight enough to encrypt large videos. Actually, various techniques are there to encrypt the images individually. But, these image encryption techniques are not used to secure videos. Video can be treated as sequence of frames. By using image encryption techniques over video to encrypt the video will provide high security along with less overhead. Here, we are converting video sequences into various frames and those frames are encrypted by using the proposed technique to attain the security. Then, again those frames are converted back to video sequence so that encrypted video sequence can be generated and can be transmitted over the wireless networks.

2. Literature Review

In recent years, many encryption techniques have been proposed to secure multimedia content. There are a lot of algorithms to secure images. But, here is the listing of some light weight image encryption techniques.

Chen C.S. and Chen R.J. [1] proposed a technique of Image encryption by pixel permutation using SCAN patterns which was encrypting images using pixel permutation.

There was one more technique of image encryption proposed by Panduranga H.T. and Kumar N.[2] which was using hybrid technique of SCAN methodology and carrier image generation from alphanumeric keyword using 4 out of 8 codes. Then, this generated carrier image is added to the actual image to generate the encrypted image.

One another technique proposed by Rajpurohit J. and Khunteta A. [3] treats the video as sequence of ordered frames running in a sequence. This algorithm first breaks the video into ordered sequence of frames and doing internal scrambling. After scrambling the frames, again the video sequence is generated.

After studying the above mentioned three techniques, the basic idea for the proposed technique arises in the mind.

3. Proposed Work

Proposed process treats video as a sequence of frames running together [3], and in first step there is conversion of video into frames. Then, encrypting those image sequences by using the image encryption techniques, pixel permutation [1] and Carrier image generation [2] in some different way. Detailed algorithm is mentioned below:

(i) Encryption Process
Inputs: Video to Encrypt & Password

1. Convert video into sequence of frames [3].
2. Calculate size of the frame.
3. Generate carrier image of image size calculated in step-2, according to the provided password [2].
4. Add original + carrier for every frame sequence.
5. Use scan patterns[1] as:
   (i) For odd sequences: scan from bottom right to top left.
   (ii) For even sequences: scan from top left to bottom right.
6. Construct video again.
7. Transmit the video over network.

Then, this video is made available to transmit over the wireless network. Even if this video is eavesdropped, then also the eavesdropper will not be able to see or watch the video content.

After receiving the encrypted video at receiver side, the decryption process will include again the conversion of video to frames, then decrypting individual frames, and constructing back the video again using decrypted frames.

(ii) **Decryption Process**
Inputs: Video to Decrypt & Password

1. Convert video into sequence of frames [3].
2. Calculate size of the frame.
3. Use scan patterns as[1]:
   (i) For odd sequences: scan from bottom right to top left.
   (ii) For even sequences: scan from top left to bottom right.
4. Generate carrier image of image size calculated in step-2, according to the provided password [2].
5. Subtract original - carrier for every frame sequence.
6. Construct video again.
7. Use the video.

4. Simulation Environment

For encryption and decryption, MATLAB v7.0 is used and for simulating the transmission over wireless networks, NS2 is used. Video sequence used for entire simulation is “FOREMAN”, foreman_qcif then converted to foreman_qcif.mp4.
Total number of frames: 400
Height: 176; Width: 144
Frame rate: 30 frames/second.

5. Simulation Parameters

a) **Encryption Quality [4]** – can be observed by Histogram Curves are used to observe the encryption quality by calculating the histogram for the provided image and histogram plot is drawn.

b) **Security Analysis (Statistical and Differential Attacks)**
   (i) *Statistical Attack Analysis* [1] – It refers to change in complete image pixel values. *Correlation Coefficient* factor is used to compute the relationship among original image and its encrypted image. This parameter shows that how much the proposed algorithm can defy statistical attacks. Consequently, encrypted image must be totally dissimilar from the original image.
   (ii) *Differential Attack Analysis* [5] – Change in some portion of video. To check the sway of changes on single pixel manipulation on the complete cipher image by the projected algorithm, these parameters are used.
   1. *NPCR - Number of Pixel Change Rate*
   2. *UACI - Unified Average changing intensity*

c) **Entropy Test [6]** – Entropy of image is a scalar value. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. It must be closer to 8 if it is encrypted.

6. Results and Discussion

1. Encryption Quality

Histogram curves for frame sequences 1, 100, 200, 300, 400 are shown below: Figure(a) shows

Frame 1:

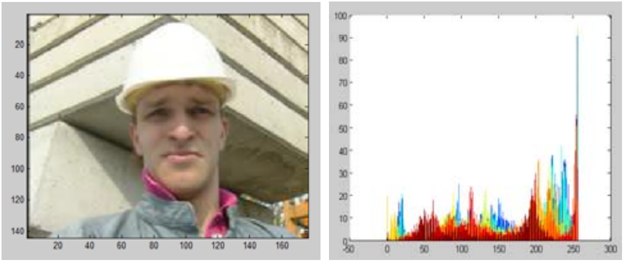

Figure (a) Original **Figure** (b) Histogram

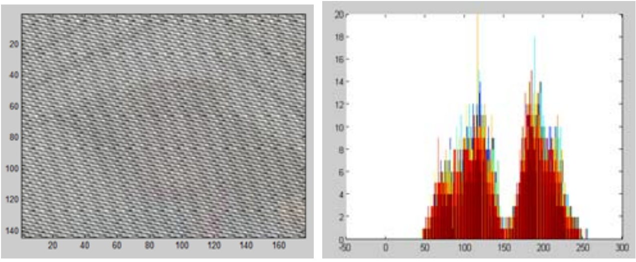

Figure (a)Encrypted **Figure** (b) Histogram

Frame 100:

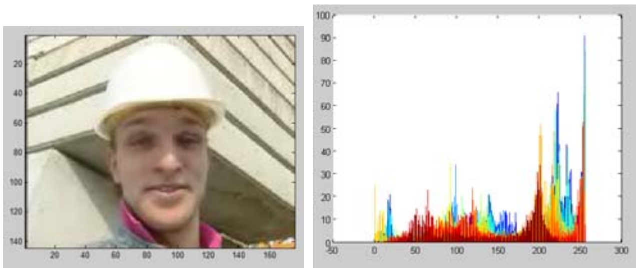

Figure (a) Original **Figure** (b) Histogram

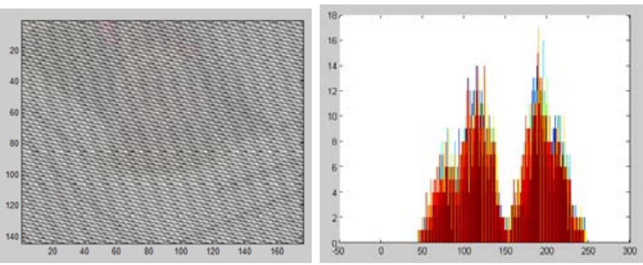

Figure (a)Encrypted **Figure** (b) Histogram

Frame 200:

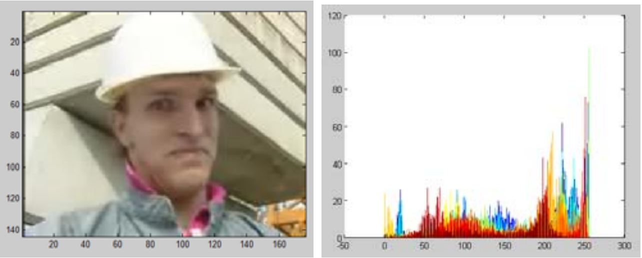

Figure (a) Original **Figure** (b) Histogram

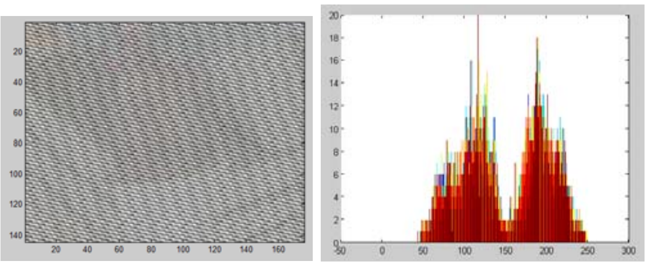

Figure (a) Encrypted **Figure** (b) Histogram

Frame 300:

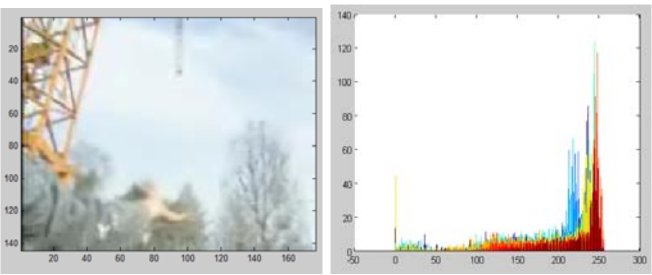

Figure (a) Original **Figure** (b) Histogram

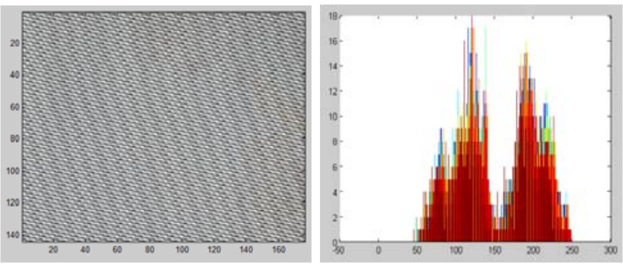

Figure (a) Encrypted **Figure** (b) Histogram

Frame 400:

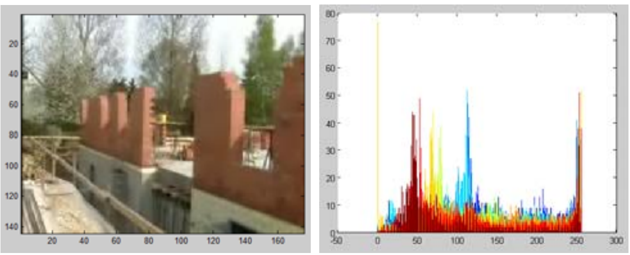

Figure (a) Original **Figure** (b) Histogram

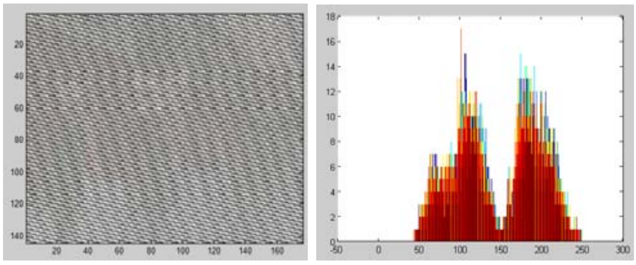

Figure (a) Encrypted **Figure** (b) Histogram

7. Security Analysis

a. Statistical Analysis

i. Correlation Coefficient

Table-1 shows the correlation coefficient values of SCAN Pattern Based Technique [1], Carrier Image Based [2], Image Scrambling Algorithm [3] and Proposed Technique. If two frames are same then CC comes out to be 1, if no relation between the frames then it comes out to be 0 and, if value is near to -1, this means the cipher image is the completely different from the original.

Table 1

Frame Sequences	*SCAN Pattern Based Technique [1]*	*Carrier Image Based[2]*	*Image Scrambling Algo[3]*	*Proposed Technique*
1	0.184262	0.258119	0.441758	0.130639
50	0.186805	0.251873	0.046888	0.001241
100	0.148196	0.260935	0.622544	-0.02279
150	0.224026	0.25399	0.689789	-0.02384
200	0.174188	0.259451	0.449793	-0.0051
250	0.158752	0.268438	0.565148	-0.03906
300	0.007717	0.17198	-0.02708	-0.01743
350	0.11097	0.24722	0.783048	0.004136
400	0.219475	0.253721	0.434411	-0.00251

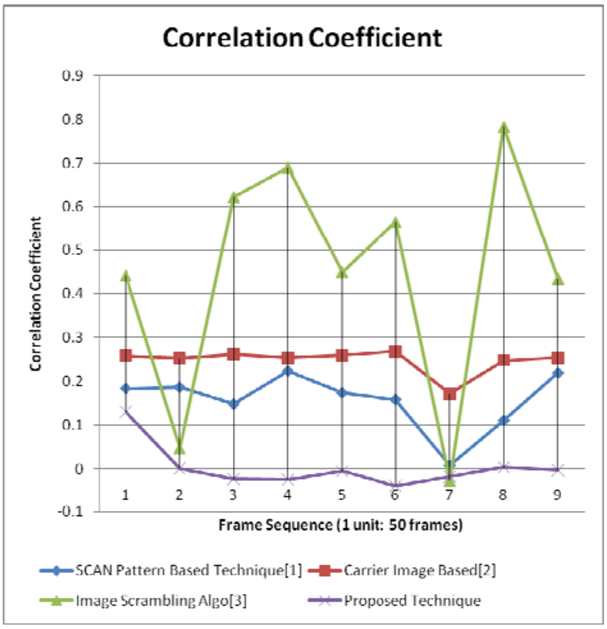

Figure-1

b) Differential Analysis

(i)NPCR

In this section, the NPCR values for two images original and encrypted are calculated. Higher values are better.

Table 2

Frame Sequences	*SCAN Pattern Based Technique [1]*	*Carrier Image Based[2]*	*Image Scrambling Algo[3]*	*Proposed Technique*
1	0.970920139	0.99402883	0.969973169	0.995699179
50	0.996501473	0.994804819	0.963041877	0.995764941
100	0.993949916	0.995225694	0.972195918	0.996146359
150	0.994436553	0.995278304	0.969552294	0.996041141
200	0.992134891	0.995107323	0.99375263	0.995094171
250	0.981442024	0.99542298	0.986019045	0.994870581
300	0.992700442	0.996120055	0.996922348	0.99950021
350	0.993344907	0.995462437	0.993489583	0.993502736
400	0.957294297	0.994489162	0.959859007	0.99313447

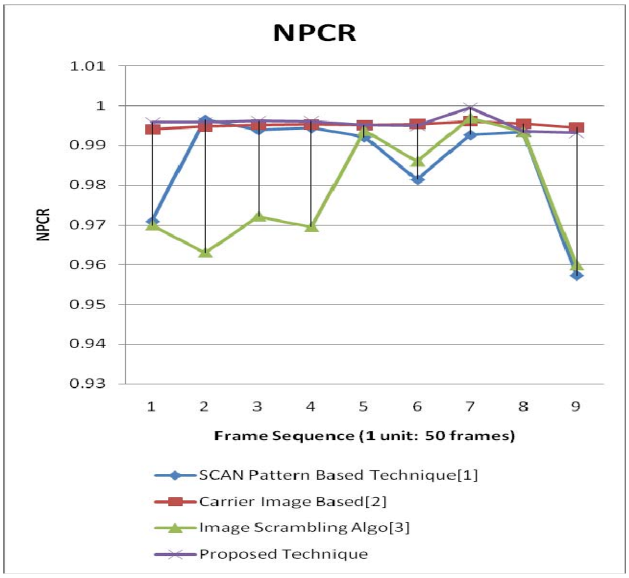

Figure-2

(ii)UACI

Similar to NPCR test, the UACI test derived in this section is also with respect to two ideally encrypted images.

Table 3

Frame Seque-nces	*SCAN Pattern Based Technique [1]*	*Carrier Image Based[2]*	*Image Scrambling Algo[3]*	*Proposed Technique*
1	0.150869603	0.23964502	0.153935288	0.306148598
50	0.31143306	0.253031696	0.121669256	0.298865493
100	0.233635425	0.26378728	0.147291801	0.318042094
150	0.306351041	0.259393516	0.138097839	0.310267091
200	0.269881928	0.258044704	0.228058	0.307166075
250	0.157701453	0.271026905	0.17930046	0.316346935
300	0.255276571	0.262057617	0.369741739	0.437670568
350	0.233635941	0.256851346	0.222933945	0.212836185
400	0.077993837	0.260319803	0.075185474	0.215882477

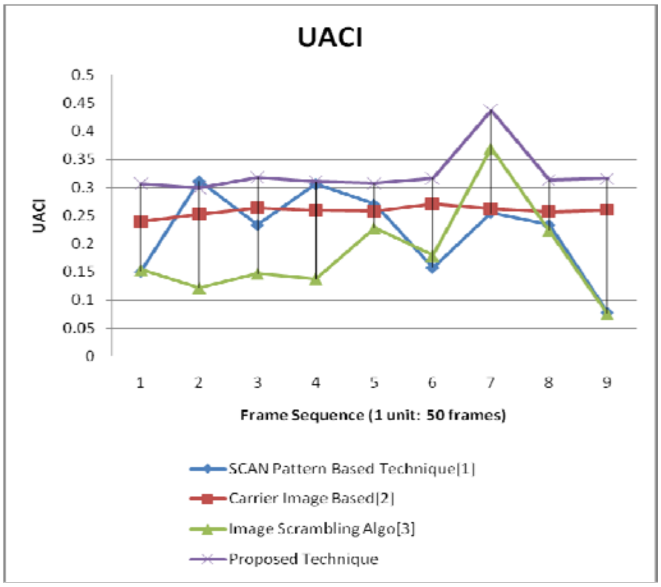

Figure 3

(iii) Entropy Test

Table-4 represents the values of entropy, value of randomness. These values must be closer to 8 if the encryption process is done.

Table 4

Frame Sequences	*SCAN Pattern Based Technique [1]*	*Carrier Image Based[2]*	*Image Scrambling Algo[3]*	*Proposed Technique*
1	7.666564	6.553606	7.591928	7.977092
50	7.596147	6.548763	7.565918	7.977057
100	7.801053	6.557192	7.571268	7.982291
150	7.590864	6.553693	7.691163	7.978993
200	7.746909	6.55212	7.754187	7.980794
250	7.269876	6.561071	7.59686	7.991096
300	7.769546	6.487614	7.617197	7.878883
350	7.695123	6.539858	7.739443	7.968876
400	7.794203	6.544587	7.584807	7.975952

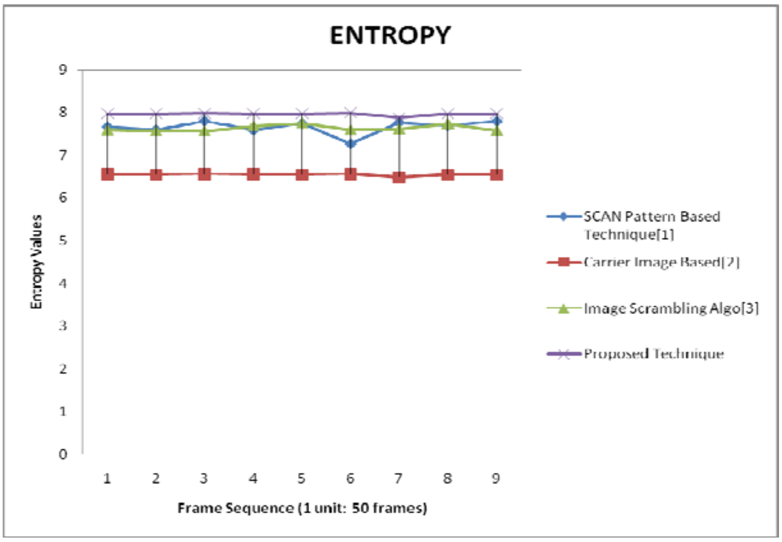

Figure 4

After observing the histogram curves we can specify the encryption quality. Low values of correlation coefficient shows proposed technique is better. Entropy test comes out to be near to 8. NPCR and UACI values shows to how much extent, the proposed technique can defy the differential attacks. Average PSNR, PLR and throughput shows better results when the video was transmitted over wireless network.

The two basic attacks are to be considered; Statistical as well as differential. Statistical analysis is done by analyzing the Correlation Coefficient. Correlation Coefficient comes out to be lower values nearby 0 and -1 which are quite satisfactory. Differential Attacks are analyzed by NPCR and UACI values. NPCR values are near to 1 which shows higher number of pixel changes, which we basically require in successful data encryption. And, UACI values are coming closer to the ideal values of 0.31 which is considered as the standard values for any media content successfully encrypting its data.

8. Conclusions

Two basic techniques were analyzed, first, encryption method to secure images using the scan based encryption process which implements pixel permutation to secure the image, second, images encryption process using the carrier image generation from alphanumeric keyword sequence using 4 out of 8 codes. On the basis of above two light weight image encryption techniques, a new technique for encrypting the images is proposed.

And on the basis of one more technique, which treat the video sequence as a sequence of running images at a particular speed. The images used in this technique are encrypted using the proposed light weight image encryption technique. Using light weight techniques of image encryption, a new technique is proposed which is better than previous techniques with less overhead. And, implementing this technique over video sequences, it provided multiplier effect of security. Individual frame is secure enough. So, the video is definitely safe from hacker attacks, eavesdropping, statistical and differential attacks.

9. Future Work

Various parameters have been successfully studied. But, if these results can be achieved by encrypting the limited number of frames then it will be much better in terms of processing time and memory requirements. Currently only one iteration is done over the sequences. More security factors can be achieved if number of iteration is increased, to encrypt the video sequences.

References

[1] Chen C.S., and Chen R.J. 2006 Image Encryption and Decryption Using SCAN Methodology *Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies*

[2] Panduranga H.T. and Kumar N. 2010 Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images. *(IJCSE) International Journal on Computer Science and Engineering* Vol. 02, No. 02, 2010, 297-300

[3] Rajpurohit J. and Khunteta A. 2013 A Scalable Frame Scrambling Algorithm for Video Encryption *Proceedings of 2013 IEEE Conference on Information and Communication Technologies.*

[4] Zhang Y., 2013 Encryption Speed Improvement on -An Improvement over An Image Encryption Method Based on Total Shuffling, *IEEE*

[5] Eslami Z., and Bakhshandeh A. 2013 An improvement over an image encryption method based on total shuffling. *Optics Communications –Elsevier*

[6] Yue Wu, Noonan, J.P., and Agaian, S. 2011 A novel information entropy based randomness test for image encryption. *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference*

[7] Chih-Heng Ke, and Wen-Shyang Hwang EVALVID - A Novel Realistic Simulation Tool for Video Transmission over Wireless Network

[8] Yue Wu, 2011 NPCR and UACI Randomness Tests for Image Encryption *Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011*