IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

A Novel Approach based on Encryption Scheme under Audio Video Steganography

Deepika Bala[1], Baldip Kaur[2], Jasdip Kaur[3]

Lala Lajpat Rai Institute of Engineering and Technology, Moga, Punjab[1,2]

North West Institute of Engineering and Technology, Dhudhike, Moga, Punjab[3]

Abstract: Steganography is process of hiding secret information behind any image and video file for the secure transmission of data. Image steganography is used for hiding information in the form of text and images. But due to lack of security reason and early detection of hiding information video steganography has been come into utilization. Video steganography comprises various frames in a single video file from which prediction of secret data availability is not come so easy process. In video steganography various frames has been extracted from a video file and secret information has to be embedded in these frames for transmission of video file.

Keywords: Stegnography, Image Stegnography, image compression, video stegnography.

1. INTRODUCTION

Steganography is the practice of hiding a document; message, picture, or feature inside an alternate record, message, picture, or video. Before, individual's utilized concealed tattoos or imperceptible ink to pass on steganography content. System advancements give simple to-utilize correspondence channels for steganography. Basically, the data concealing process in a steganography framework begins by recognizing a cover medium's repetitive bits (those that can be adjusted without wrecking that medium's trustworthiness). The inserting methodology makes a steno medium by replacing these excess bits with information from the hidden message. Present day steganography objective is to keep its minor presence imperceptible, yet steganography frameworks as a result of their obtrusive nature desert discernible follows in the spread medium. Regardless of the possibility that mystery substance is not uncovered, the presence of it is changing the spread medium changes its factual properties, so busybodies can catch the mutilations in the subsequent stego medium's measurable properties. The methodology of discovering these twists is called factual steganalysis (Guo, 2007). A standout amongst the most broadly utilized applications is for supposed computerized watermarking. A watermark, verifiably, is the replication of a picture, logo, or content on paper stock with the goal that the wellspring of the report can be in any event incompletely confirmed. A computerized watermark can finish the same capacity; a visual craftsman, for instance, may post specimen pictures on her webpage complete with an installed mark so she can later demonstrate her possession in the event that others endeavor to depict her role as their own. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of our cat could conceal the plans for our company's latest technical innovation (Alla, 2009).

2. REVIEW OF LITERATURE

Alla, K. et al [1] "An Evolution of Hindi Text Steganography" Author was presented a novel steganography scheme suitable for Hindi text. It can be classified under text steganography. Conveying information secretly and establishing a hidden relationship between the message and its counterpart has been of great interest since very long time ago. Methods of steganography are mostly applied on images, audio, video and text files. During the process characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Text documents are the best examples for this. This paper presents a novel Hindi text steganography, which uses Hindi letters and its diacritics and numerical code. This method is not only useful to Hindi text but also to all other similar Indian languages.

Gupta, Rupesh et al [2] "New proposed practice for secure image combing cryptography steganography and watermarking based on various parameters" Since the ascent of utilization of web on the planet security is turning into

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

the real concern everywhere. So making this thing clear at the top of the priority list engineers are consistently attempting to make web a safe domain for all the clients. Numerous calculation or procedures are proposed and they worked yet as the gatecrashers are acting insightfully to hack data engineers are likewise expected to create new methods to stop programmer's propositions. According to the fundamental information more is the PSNR quality and lesser is the MSE results are better along these lines, here in this paper author proposing another strategy by brushing three noteworthy security methods that is cryptography, steganography and watermarking that won't just shroud the data yet deliver better results for MSE. PSNR and Embedding limit still after the clamor assault. The reason this paper is to give another strategy that will give better security to concealing information in a picture and watermarked feature.

Amirtharajan et al [3] "An evaluation of image based steganography methods" Author use one component case: here we have 3 ways to determine the bits * 3 ways to decide the component R, G or B. this results in 9 cases. Using two component case: here we have 3 ways to determine the bits * 3 ways to decide the component RG, RG or GB. This results in 9 cases. Using three component case: here we have 3 ways to determine the bits * one way to decide the component which is RGB. This results in 3 cases. The average capacity ratio is around 1/7 or 14% of the original cover media size. The secret data is scattered throughout the whole image. Also, extracting the secret data without the knowledge of seeds is almost impossible. The capacity of the triple technique is higher than the previous techniques. By using this algorithm, the ratio between the number of bits used inside a pixel to hide part of the secret message; and the number of bits in the pixels itself, which is defined as the capacity factor can be in the range from 1/24 to 9/24 if we use a maximum of 3 bits. Moreover, if we extend the algorithm to hide 4 and even 5 bits the factor can be increased up to 15/24 which is above half of the pixel bits, but the down side is the additional noise introduced as the number of bits used to hide the secret data increase.The algorithm adds more randomization by using two different seeds generated from a user-chosen key in order to select the component(s) used to hide the secret bits as well as the number of the bits used inside the RGB image component. Thus the disadvantage of this technique is its key management.

Mehdi Hussain et al [4] "Pixel Intensity Based High Capacity Data Embedding Method" Steganography is the art of concealing a message signal to have signal, with no bending in the facilitated sign. Utilizing steganography, data can be covered up in facilitated transporter, for example, pictures, features, and sounds records, content documents, and information transmission. In picture steganography, to enhance the limit of concealed information into facilitated picture without creating any factually noteworthy adjustment has a real concern. Numerous novel information concealing strategy taking into account Least Significant Bits (LSB) and Pixel Value Differencing (PVD) to build the concealing limit have been proposed with subtle quality. This paper has enhanced the Modified Kekre's Algorithm (MKA) which is taking into account LSB system. The enhanced plan builds the implanting limit while holding the great nature of stego-picture (convey concealed information) as good as MKA. Trial results demonstrate that the enhanced plan outflank the first near plan particularly in limit of concealed information bits.

Asad, M et al [5] "An enhanced least significant bit modification technique for audio steganography" Expanded utilization of electronic correspondence has conceived better approaches for transmitting data safely. Audio steganography is the exploration of concealing some mystery content or sound data in a host message. The host message before steganography and stego message after steganography have the same attributes. Least Significant Bit (LSB) change method is the most basic and productive system utilized for sound steganography. The traditional LSB alteration procedure is defenseless against steganalysis. This paper proposes two approaches to enhance the traditional LSB change strategy. The primary path is to randomize bit number of host message utilized for implanting mystery message while the second route is to randomize specimen number containing next mystery message bit. The extemporized proposed procedure conflicts with steganalysis and declines the likelihood of mystery message being extricated by an interloper. Advanced Encryption Standard (AES) with 256 bits key length is utilized to secure mystery message on the off chance that the steganography method breaks.

3. METHDOLOGY

Take a video file as cover file. A separator is used to separate the audio & video files. In Audio, the phase coding approach is applied. After that we get stego audio**.** In video, the frame extraction is used. Then MLSB approach is used. After that we get stego video is used.

Figure 3.1 represents flow of the proposed work embedding of secret information behind cover audio and video files. In this flow chart various steps has been described that has been used for embedding of secret information behind cover files. Firstly a video file has been taken as a cover object and that has been preprocessing using Audio-Video separator. Audio video separator used for separation of audio and video information has extracted from a single video file. After division of video file data has been embedded behind the audio and video files using embedding approaches. After embedding of secret information behind video and audio files different stego files have been recombine to form a stego video file.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

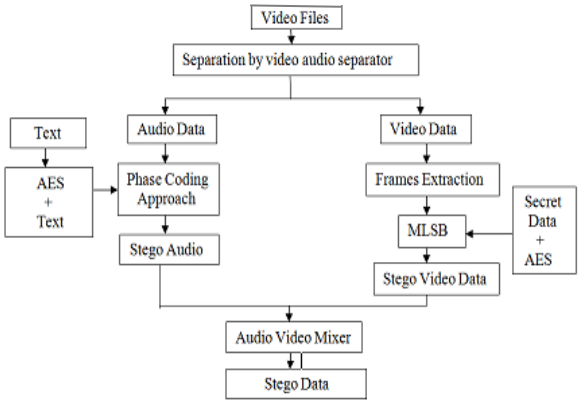

Fig 3.1 Flow of embedding secret information behind audio and video file

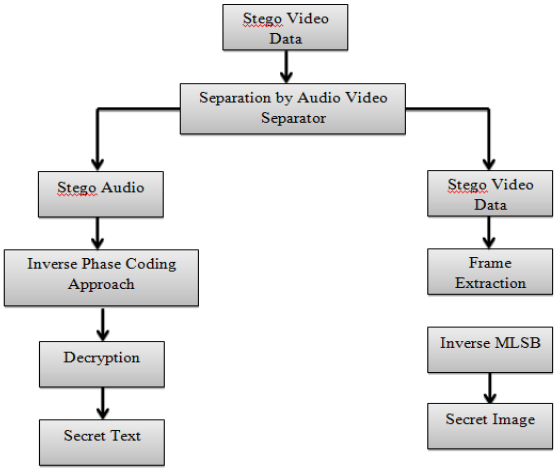

Fig 3.2 Flow of Extraction of secret information from audio and video file

Figure 3.2 represents flow of the proposed work for extraction of secret information from the stego file by separation of the stego video to stego audio and stego video data. After conversion of these files data has been extracted by using decryption approaches.

4. RESULTS

Table 4.1 PSNR for different videos using proposed and previous approach for 32*32 image size

Video	Proposed	Previous
Video 1(640*360)	59.62 dB	47.54 dB
Video 2(640*272)	58.37 dB	46.34 dB
Video3(640*360)	59.61 dB	47.58 dB
Video 4(640 *360)	59.59 dB	47.98 dB
Video 5(854*480)	51.74 dB	48.36 dB
Video 6(854*480)	61.90 dB	49.67 dB
Video 7(854*480)	62.14 dB	43.77dB
Video 8(854*480)	62.11 dB	50.01 dB
Video 9 (854*480)	62.13 dB	50.03 dB
Video 10(854*480)	62.10 dB	50.23dB

Table 4.1 describes PSNR values for various video files that have been used for embedding of secret information. PSNR represents peak signal noise ratio provides information about distortion occurred into cover object after embedding of secret information. This table represents values of PSNR computed on embedding secret information of 32 X 32.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

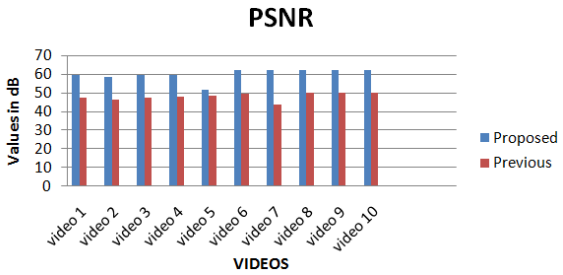

Fig 4.1 Graphical Representation for PSNR

Figure 4.1 represents value of PSNR for distortion occurred in the video after embedding of secret information of 32 X 32.

Table 4.2 MSE for different videos using proposed and previous approach for 32*32 image size

Video	Proposed	Previous
Video 1	0.07	1.14
Video 2	0.07	1.50
Video 3	0.07	1.13
Video 4	0.43	1.03
Video 5	0.43	0.94
Video 6	0.04	0.70
Video 7	0.03	0.72
Video 8	0.03	0.64
Video 9	0.03	0.64
Video 10	0.04	0.61

Table 4.2 describes MSE values for various video files that have been used for embedding of secret information. In the purposed work Mean Square Error represents error occurred in cover object after embedding secret information. Low value of MSE represents low distortion occurred in cover file. MSE has been computed for different video files by embedding secret information of 32 *32.

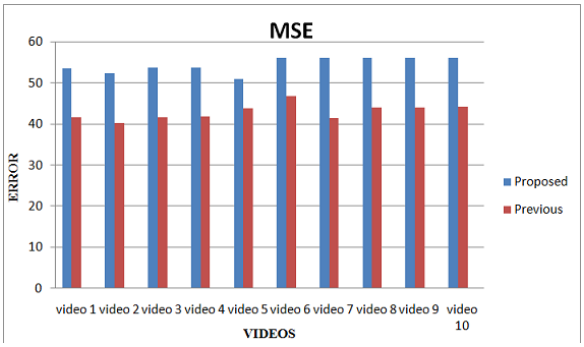

Fig 4.2 Graphical Representation for MSE

Figure 4.2 represents value of MSE for distortion occurred in the video after embedding of secret information. Lower value of MSE represents less distortion occurred in the network.

Table 4.3 PSNR for different videos using proposed and previous approach for 64*64 image size

Video	Proposed	Previous
Video1(640*360)	53.56 dB	41.54 dB
Video2(640* 272)	52.36 dB	40.27 dB
Video 3 (640* 360)	53.59 dB	41.51 dB
Video 4 (640 * 360)	53.61 dB	41.72 dB
Video 5 (854* 480)	50.93 dB	43.84 dB
Video 6(854* 480)	56.07 dB	46.65 dB

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

Video 7 (854* 480)	56.10 dB	41.45 dB
Video 8(854* 480)	56.06 dB	43.99 dB
Video 9 (854* 480)	56.08 dB	44.03 dB
Video 10 (854* 480)	56.10 dB	44.19 dB

Table 4.3 describes PSNR values for various video files that have been used for embedding of secret information. PSNR represents peak signal noise ratio provides information about distortion occurred into cover object after embedding of secret information. This table represents values of PSNR computed on embedding secret information of 64*64.

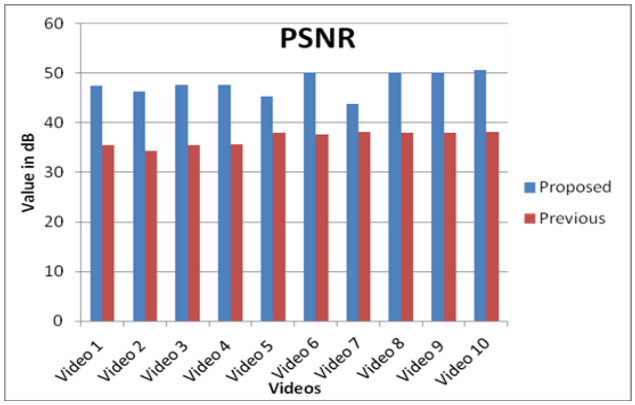

Fig 4.3 Graphical Representation for PSNR

Figure 4.3 represents value of PSNR for distortion occurred in the video after embedding of secret information. Higher value of PSNR represents less distortion occurred in the network. Table 5.4 MSE for different videos using proposed and previous approach for 64*64 image size.

Table 4.4 MSE for different videos using proposed and previous approach for 64*64 image size.

Video	Proposed	Previous
Video 1	0.28	4.56
Video 2	0.37	6.09
Video 3	0.28	4.58
Video 4	0.28	4.36
Video 5	0.52	2.68
Video 6	0.16	2.80
Video 7	0.15	4.65
Video 8	0.16	2.59
Video 9	0.16	2.56
Video 10	0.15	2.47

Table 4.4 describes MSE values for various video files that have been used for embedding of secret information. In the proposed work Mean Square Error represents error occurred in cover object after embedding secret information. Low value of MSE represents low distortion occurred in cover file. MSE has been computed for different video files by embedding secret information of 64*64.

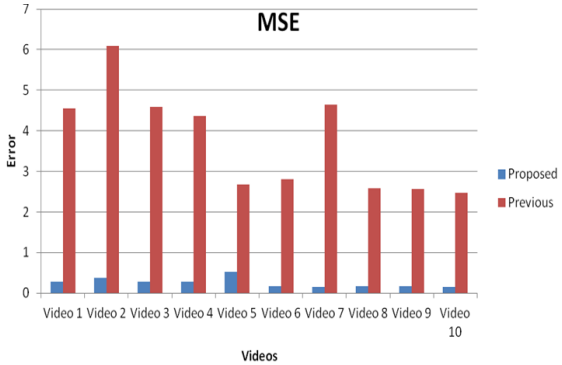

Fig 4.4 Graphical Representation for MSE

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

Figure 4.4 represents value of MSE for distortion occurred in the video after embedding of secret information. Lower value of MSE represents less distortion occurred in the network.

Table 4.5 SSIM for different videos using proposed and previous approach for 32*32 image size

Video	Proposed	Previous
Video1(640*360)	0.99	0.96
Video2(640*272)	0.98	0.95
Video3(640*360)	0.99	0.97
Video4(640 *360)	0.99	0.98
Video5(854*480)	0.99	0.97
Video6(854*480)	0.99	0.97
Video7(854*480)	0.99	0.97
Video8(854*480)	0.99	0.96
Video9(854*480)	0.99	0.97
Video10(854*480)	0.98	0.97

Table 4.5 describes SSIM values for various video files that have been used for embedding of secret information. SSIM structure similar index matrix that provides information about changes in structure occurred into cover object after embedding of secret information. This table represents values of SSIM computed on embedding secret information of 32*32.

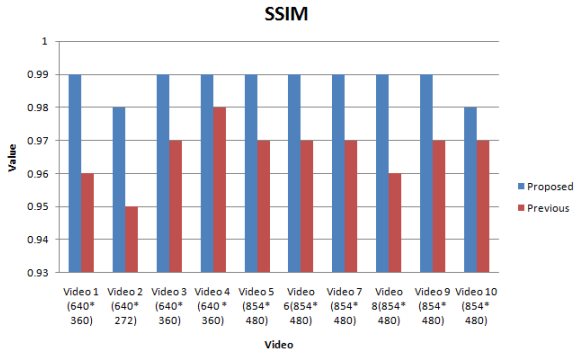

Fig 4.5 Graphical Representation for SSIM

Table 4.6 Correlation for different videos using proposed and previous approach for 32*32 image size

Video	Proposed	Previous
Video1(640*360)	0.98	0.92
Video2(640*272)	0.98	0.92
Video3(640*360)	0.99	0.92
Video4(640*360)	0.99	0.93
Video5(854*480)	0.99	0.97
Video6(854*480)	0.99	0.92
Video7(854*480)	0.99	0.89
Video8(854*480)	0.99	0.92
Video9(854*480)	0.99	0.96
Video10(854*480)	0.99	0.96

Table 4.6 describes correlation values for various video files that have been used for embedding of secret information. Correlation that provides information about changes correlation coefficients occurred into cover object after embedding of secret information. This table represents values of SSIM computed on embedding secret information of 32 X 32.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 6, June 2018

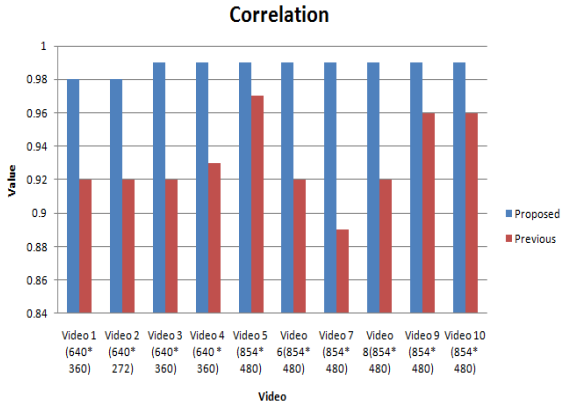

Fig 4.6 Graphical Representation for CC

5. CONCLUSION & FUTURE SCOPE

Video Steganography is emerging field for secure transmission of secret information over the communication channels. Steganography is used to hide secret information behind cover object so that data can be transmitted in secure manner such that does not see through naked eyes. Video Steganography is related to hiding information behind the frames of the video file that can't be extracted easily without information of frames content. In the proposed work video steganography has been done to hide information in such a manner so that data can be transmitted in secure manner. In the proposed work audio and video steganography is used for authentication purpose. In this research an approach has been used that utilize video hidden data as authentication message. In this process audio and video has been extracted from a video file using separator. Audio file is used for hiding text message that has been encrypted using AES approach and video file is used to hide secret image after encryption using bit shifting approach. MLSB and phase coding approach has been used for hiding of secret information behind video and audio data respectively. In this thesis an encrypted based steganography approach has been proposed that used for hiding data behind audio and video content of single file and combines these files to transmit over the network to receiver end. After extraction of video hidden information authentication of the data has been validated. On the basis of authentication audio hidden information can be extracted. In the proposed work various parameters that are peak signal to noise ratio and mean square error has been performance evaluation of proposed work. As we can analyze from the results that proposed approach is much better than previous approach in terms of security and distortion after embedding. In the future reference the proposed approach can be used in real world application so that security can be provided for secret information.

The proposed model can be enhanced on the basis of utilization of artificial intelligence approaches so that region can be extracted that can be used for data embedding.

REFRENCES

[1] Alla, K., Prasad, R. "An Evolution of Hindi Text Steganography" Sixth International Conference onInformation Technology: New Generations, 2009, pp. 1577 – 1578.
[2] Moon, S.K, Kawitkar, R.S., "Data Security Using Data Hiding", IEEE International Conference on Computational Intelligence and Multimedia Applications, vol. 4, pp. 247-251, 2007.
[3] Mathkour, H, Al-Sadoon, B., Touir, A. "A New Image Steganography Technique" IEEE 4th International Conference onWireless Communications, Networking and Mobile Computing, pp.1-4, 2008.
[4] Mehdi Hussain, MureedHussain, "Pixel Intensity Based High Capacity Data Embedding Method", IEEE International Conference onInformation and Emerging Technologies, pp. 1-5, 2010
[5] Asad, M, Gilani, J., Khalid, A., "An enhanced least significant bit modification technique for audio steganography", IEEE International Conference onComputer Networks and Information Technology, pp. 143-147, 2011
[6] Karaman, H.B,Sagiroglu, S. "An Application Based on Steganography" IEEE International Conference onAdvances in Social Networks Analysis and Mining, pp. 839-843, 2012.
[7] Saravanan, V, Neeraja, A. "Security issues in computer networks and steganography", IEEE 7th International Conference onIntelligent Systems and Control, pp. 363-366, 2013.
[8] XikaiXu, Wei Wang, Tieniu Tan, "Video steganalysis based on the constraints of motion vectors", 20th IEEE International Conference onImage Processing, pp. 4422-4426, 2013.
[9] Banerjee, S, Chakraborty, M.S., Das, S. "A variable higher bit approach to audio steganography" IEEE International Conference onRecent Trends in Information Technology, pp. 46-49 and 2013.
[10] Ramaiya, M.K, Hemrajani, N., Saxena, A.K. "Security improvisation in image steganography using DES" IEEE 3rd InternationalAdvance Computing Conference, pp. 1094-1099, 2013
[11] Gupta, Rupesh, TanuPreet, "New proposed practice for secure image combing cryptography stegnography and watermarking based on various parameters", IEEE International Conference onContemporary Computing and Informatics, pp. 475-479, 2014.
[12] Md. Rashedul Islam, AyashaSiddiqa, Md. PalashUddin, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", IEEE 3rd International Conference on Informatics, Electronics & Vision, pp. 1-6, 2014.