British Journal of Mathematics & Computer Science
7(3): 218-228, 2015, Article no.BJMCS.2015.117
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Robust Electronic Communication Scheme in Spatial Domain

Aqsa Rashid[1*]

[1]Department of Computer Science and Information Technology, The Islamia University of Bahawalpur, Pakistan.

Article Information

DOI: 10.9734/BJMCS/2015/15228
Editor(s):
(1) Victor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
Reviewers:
(1) Rajlaxmi Nair, Electronics & Communication Engineering, V.T.U, India.
(2) Yong Zhang, School of Software and Communication Engineering, Jiangxi University of Finance and Economics, China.
(3) Anonymous, India.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=934&id=6&aid=8128

Original Research Article

Received: 14 November 2014
Accepted: 27 January 2015
Published: 14 February 2015

Abstract

With the growing tempo of not permitted right to use and assail, protection of private facts is of extreme value. These concerns results in Steganography. Simple least significant bit matching and least significant bit substitution techniques and some other methods have an advantage that after hiding the message, the distortion and statistical change in image is least. The purposed method uses the advantages of these methods and removes the negative aspect connected with them. Theoretically and practically, it is very difficult to break the proposed method. It is implemented for both the grayscale and color images.

Keywords: LSB, robust, secured, steganography.

1 Introduction

In last few years, due to the encroachment in technology and the increase swiftly of data broadcast, most inhabitants have a preference to use the internet as the important middling to convey data. The data conduction is made very straightforward, quick and precise via the internet. On the other hand, the fortification and protection has become an important issue in the digital world.

**Corresponding author: aqsarashid2@gmail.com;*

In current era, Steganography is measured as a gifted approach for secure electronic communication. It is the science of hiding information in such a way that its existence cannot be noticed. Image steganographic process involves two files. The initial is the image that will clasp the concealed data known as cover image. The subsequent file is the data - the secret information to be concealed. The joint image is called a stego-image. Experimentally, it is examined that accumulation of the message inside an image creates a change in statistics. If this change is very small it cannot be detected.

In the recent year numerous looms, schemes and systems of image steganographic have been urbanized to defend our secret information while transferring from foundation to target techniques [1,2,3,4,5,6] have been projected. Some spatial domain with their advantages and limitations are discussed below:

LSB substitution [7] is the flipping method. It replaces the least significant bit of pixel with message bit. If the pixel's least significant bit and message bit are identical then no replacement is required. This replacement creates a least change in the image visual and statistical properties of the image.

LSB matching [8,9] is similar to that of LSB substitution with the difference being that for making the least significant bit the message bit, it does not replace the pixel bit with the message bit. Instead it increment or decrement the pixel value by one in such a manner that the least significant bit turns into the message bit.

LSB Matching Revisited [10] LSB substitution and LSB matching creates the specific sequence in the pixel value which is detectable by the histogram analysis. LSB matching revisited is the perfection of LSB matching by decrementing the change per pixel and hence removes the specific sequence and making attack difficult.

Gray Level Modification (GLM) [11] chooses the set of pixels based on some mathematical function and makes all the odd pixels to even by incrementing. Now if the message bit is 0 then nothing to be performed as the least significant bit is 0 already and if it is 1 then GLM methods simply decrement the pixel value to make pixel least significant bit 1.

Robust increased Capacity Image Steganography Scheme [12] increases the capacity for message bits with very less change in statistical properties of the image. This method uses two least significant bit of pixel. On second least significant bit the matching process is applied and on least significant bit the replacement is applied.

All these schemes are unfussy, efficient and work okay. The major problems attached with these techniques are:

- All of these utilize the least significant bit (LSB) for hiding covert message due to which message can be easily splintered by pretender by altering all the LSBs of the image.
- LSBs are more susceptible to hardware fault.

The rest of the paper is arranged as Section 2 describes the Method, Section 3 discusses the comparison tools used for analysis, Section 4 includes Experimental results and discussion, Section 5 is the conclusion and references are in last section.

2 Methods

In the proposed method, three bits next to least significant bit are used in processing. Mod value of the decimal equivalent of these three bits is computed by using 2 as a mod-factor. The mode function is calculated as follows:

$$\text{Mod-factor}=2^{m}$$

Here m is the number of bits to hide in one pixel. So, in a view of this m can be 2, 3, etc. In the purposed method m=1, such that the mod-factor would be 2. If the binary of mod value and the message bit are now the same, nothing to be done. Otherwise the adjustment is to be done by incrementing or decrementing in pixel value in such a way that the binary of mod value and message bit becomes equivalent.

Similarly for embedding two bits per pixel the mod-factor will be 4, for embedding 3 bits mod-factor will be 8 and so on.

Table 1 shows the whole process for embedding one bit per pixel. First column shows all the possibilities of the three bits next to least significant bit. Second column is the decimal of the three bits. Third column shows the mode values with the mod-factor 2. Forth column shows the message bits that can be embedded without adjustment i.e. if the mode value is 0 then only 0 can be embedded in that location without adjustment. If bit 1 is to be embedding in location where the mod value is 0 then adjustment should be performed. Similarly if the mode value is 1 then only 1 can be embedded without adjustment. Tables 2 and 3 show the similar analysis for embedding two and three bits per pixel respectively.

Table 1. One bit per pixel

Three bits	Decimal of three bits	Mode value	Message bit
000	0	0	0
001	1	1	1
010	2	0	0
011	3	1	1
100	4	0	0
101	5	1	1
110	6	0	0
111	7	1	1

Table 2. Two bits per pixel

Three bits	Decimal of three bits	Mode value	Message bit
000	0	0	00
001	1	1	01
010	2	2	10
011	3	3	11
100	4	0	00
101	5	1	01
110	6	2	10
111	7	3	11

Table 3. Three bits per pixel

Three bits	Decimal of three bits	Mode value	Message bit
000	0	0	000
001	1	1	001
010	2	2	010
011	3	3	011
100	4	4	100
101	5	5	101
110	6	6	110
111	7	7	111

2.1 Example of Purposed Method

This subsection gives the examples of proposed method for one and two bits per pixel embedding. E.1 and E.2 are the example when the mode value is 0. E.3 and E.4 are the example when the mod value is 1.

E.1:	**E.2:**
Message bit=0 Pixel decimal=21 Pixel binary= 00010101 Three bits next to least significant bit= 010 Decimal of three bits= 2 Mod value =0 Mod value and message bit are same. No adjustment is required.	Message bit=1 Pixel decimal=21 Pixel binary= 00010101 Three bits next to least significant bit= 010 Decimal of three bits= 2 Mod value =0 Mod value and message bit are not same. Pixel adjustment required in the form of increment. After adjustment pixel decimal becomes 22.

E.3:	**E.4:**
Message bit=1 Pixel decimal=118 Pixel binary= 01110110 Three bits next to least significant bit= 011 Decimal of three bits= 3 Mod value =1 Mod value and message bit are same. No adjustment is required.	Message bit=0 Pixel decimal=118 Pixel binary= 01110110 Three bits next to least significant bit= 011 Decimal of three bits= 3 Mod value =1 Mod value and message bit are not same. Pixel adjustment required in the form of decrement. After adjustment pixel decimal becomes 117.

Below are the examples of proposed method for two bit per pixel embedding. In E.5 the mod value is 0 so only 00 message bits can be embedded without adjustment. In E.6 the mod value is 1 so only 01 message bits can be embedded without adjustment.

E.5:	**E.6:**
Message bit=00 Pixel decimal=21 Pixel binary= 00010101 Three bits next to least significant bit= 010 Decimal of three bits= 2 Mod value =0 Mod value and message bit are same. No adjustment is required.	Message bit=01 Pixel decimal=118 Pixel binary= 01110110 Three bits next to least significant bit= 011 Decimal of three bits= 3 Mod value =1 Mod value and message bit are same. No adjustment is required.

2.2 Formal Steps of Proposed Method

Formal Steps for insertion process are:

Input: Cover Image CI, array of message bit stream BS

Output: Stego-image SI

a) Mine three bits (Tb) next to least significant bit (LSB) of the pixel (P).
b) Compute the mod value (m) of decimal equivalent (d) of three bits (Tb) by 2 as mod factor.

c) If the binary of mod value (m) and message bit (Mb), from bit stream (BS), are equivalent then no adjustment is required. Go to END. If NO go to next step.
d) Adjust the pixel value so that the message bit (Mb) and binary of mod value (m) become equivalent.
e) END

Formal Steps for extraction process are:

Input: Stego-image SI

Output: Array of message bit stream BS

a) Mine three bits (Tb) next to least significant bit (LSB) of the pixel (P).
b) Compute the mod value (m) of decimal equivalent (d) of three bits (Tb) by 2 as mod factor.
c) If the mod value (m) is 0 then put 0 in the bit stream (BS) else put 1 in the bit stream (BS).
d) END

These formal steps are for the grayscale image. For color image, one pixel has three components or channels namely red, green and blue. For each channels the above stated steps are to be performed.

3 Tools Used for Analysis

The section is further subdivided into two sections. First is named as “Security Analysis” [13] and second is named as “Robustness Analysis” [14,15,16,17,18].

3.1 Security Analysis

Comparing the histograms of cover image and the stego-image gives the clear idea of security. The security examination evaluates the cover image with the stego-image on the basis of histograms of Images. For histogram comparison Jaccard measure, Correlation, Chi-square, Intersection and Bhattacharya distance [13] are computed between the histogram of cover image and stego-image.

All these comparisons are performed on normalized histogram. The value of Jaccard and correlation varies between 1 and -1. Perfect match is 1 and total mismatch is -1. For Chi-square ideal value is 0 and mismatch value is unbound, for intersection 1 is ideal matching value and 0 is mismatched value and Bhattacharya distance gives 0 for the exact match and 1 for mismatch. When these comparison matrices gives ideal values or values that are closer to ideal values then the change in histogram is very least and this is the evidence for Stego-System to be a secure system.

3.2 Robustness Analysis

Robustness of any method depends on different parameters. In the paper four most important and widely used Image quality measures [14,15,16,17,18] namely MSE, PSNR, UIQI and SSIM are computed for comparison.

Mean Square Error computes the perceived error. It is pixel value difference based quality measure. Peak Signal to Noise Ratio is inversely proportional to MSE. Less MSE gives High PSNR which is the proof of the fact that image has good quality.

Image Quality Index split the judgment of similarity between Cover Image (CI) and Stego-Image (SI) into three comparisons: Luminance, Contrast and Structural Information. SSIM estimates "Perceived change in structural information". It computes the similarity between two images of common size.

The value of UIQI and SSIM varies between 1 and -1. Closer the highest positive value denotes too much less change in two images and -1 shows totally mismatch. UIQI and SSIM are considered as more consistent and accurate than MSE and PSNR.

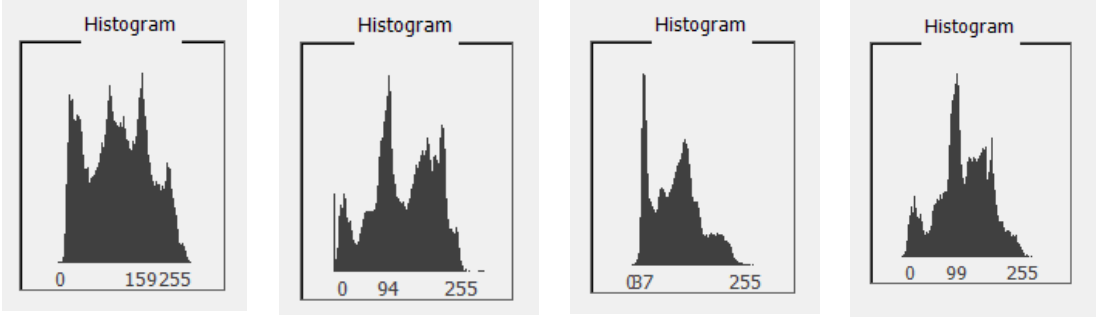
4 Experimental Results

This section presents the experimental results obtained after implementing the proposed method in .NET Framework (C#). A system is designed and implemented in. NET Framework (C#) that shows the functioning of projected Steganography method. The system is named as Secured and Robust Information Hiding Steganographic Scheme (SRIHSS) because of exceptional results of Security Analysis and Robust analysis.

The proposed method is tested on many standard images. Some from the tested database are shown in Fig. 1. (a) is the Barbara grayscale image having dimensions 512 x 512, (b) is the Pepper grayscale image having dimensions 512 x 512, (c) is the Lena color Image having dimensions 512 x 512 and (d) is the Pepper color image having dimensions 225 x 225.

Fig. 1. Images used for test

Fig. 2 shows the histogram of the Cover images, of Fig. 1, used in testing. Histogram also shows the maximum number of pixels having the same color. It is 159 in (a), 94 in (b), 37 in (c) and 99 in (d).



(a) Histogram of Barbara Gray | **(b) Histogram of Pepper Gray** | **(c) Histogram of Lena Color** | **(d) Histogram of Pepper Color**

Fig. 2. Histograms of the Cover Images (CI)

The section is also divided into two subsections. First will give the experimental results for grayscale images and second subsection will give for color images.

4.1 Grayscale Images

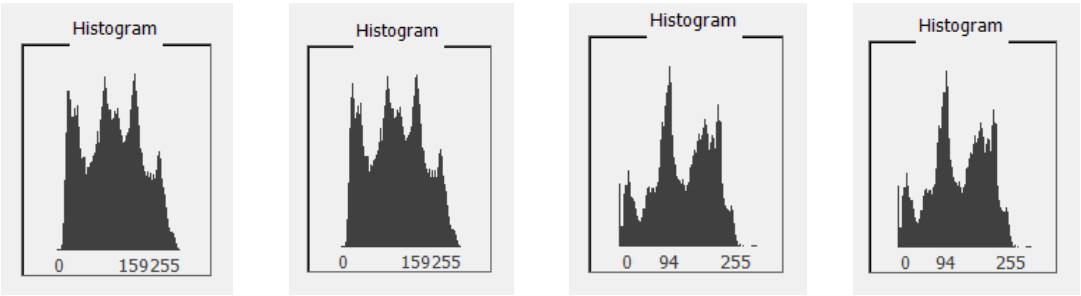
This section gives the experimental results for grayscale images. Fig. 3 shows the visual appearance of grayscale images after embedding secret message in the Barbara Gray and Pepper Gray. Fig. 3 (a) is the Stego-Barbara Gray with 81944 bits of hidden data; (b) is the Stego-Barbara Gray with 96064 bits of hidden data, (c) is the Stego-Pepper Gray with 96064 bits of hidden data and (d) is the Stego-Pepper Gray with 106992 bits of hidden data.

a) Stego-Barbara Gray with 81944 bits | **(b) Stego-Barbara Gray with 96064 bits** | **(c) Stego-Pepper Gray with 96064 bits** | **(d) Stego-Pepper Gray with 106992 bits**

Fig. 3. Stego-Gray images

Fig. 4 shows the visual appearances of the histograms of the stego-images of Fig. 3.

Histogram also shows the maximum number of pixels having that same color. It is 159 in (a), 159 in (b), 94 in (c) and 94 in (d).



(a)Histogram of Stego-Barbara Gray with 81944 bits | **(b) Histogram of Stego-Barbara Gray with 96064 Bits** | **(c) Histogram of Stego-Pepper Gray with 96064 bits** | **(d) Histogram of Pepper Gray with 106992 bits**

Fig. 4. Histograms of Stego-Gray Images

Table 4 shows the result of security analysis and robustness analysis, computed between the Barbara Gray and Stego-Barbara Gray, with 81944 bits of hidden data and 96064 bits of hidden data.

Table 5 shows the result of security analysis and robustness analysis, computed between Pepper Gray and Stego-Pepper Gray, with 96064 bits of hidden data and 106992 bits of hidden data.

Table 4. Result of security and robustness analysis for the Barbara Gray image

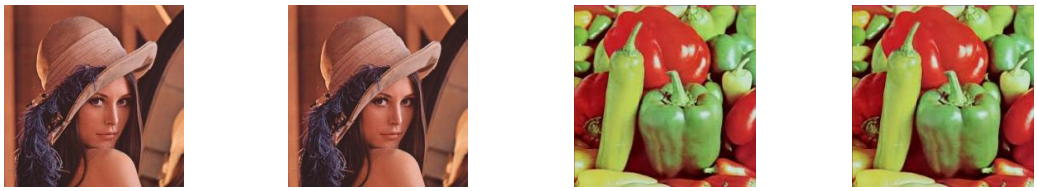
Method	81944 bits	96064 bits	Method	81944 bits	96064 bits
Jaccard	0.99999	0.99999	MSE	0.15600	0.18263
Intersection	0.99934	0.99923	PSNR	55.19929	55.51502
Correlation	0.99997	0.99997	UIQI	0.99997	0.99997
Chi-Square	0.00066	0.00078	MSSIM	0.99997	0.99997
Bhattacharya	0.00141	0.00158			

Table 5. Result of security and robustness analysis for the pepper Gray image

Method	96064 bits	106992 bits	Method	96064 bits	106992 bits
Jaccard	0.99999	0.99999	MSE	0.18263	0.20546
Intersection	0.99923	0.99913	PSNR	55.51502	55.00346
Correlation	0.99997	0.99996	UIQI	0.99997	0.99996
Chi-square	0.00079	0.00088	MSSIM	0.99997	0.99996
Bhattacharya	0.00279	0.00285			

4.2 Color Images

This section gives the experimental results for Color images. Fig. 5 shows the visual appearance of color images after embedding secret message in the Lena Color and Pepper Color. Fig. 5 (a) is the Stego-Lena Color with 81944 bits of hidden data; (b) is the Stego-Lena Color with 114744 bits of hidden data, (c) is the Stego-Pepper Color with 84336 bits of hidden data and (d) is the Stego-Pepper Color with 107008 bits of hidden data.



(a)Stego-Lena color with 81944 bit | **(b) Stego-Lena color with 114744 bits** | **(c) Stego-Pepper color with 84336 bits** | **(d) Stego-Pepper color with 107008 bits**

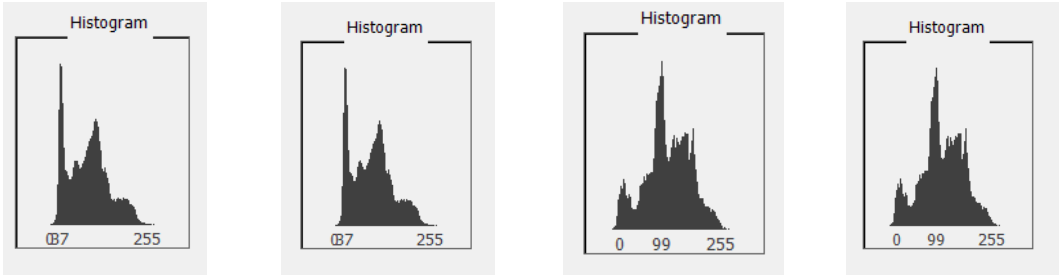
Fig. 5. Stego-Color images

Fig. 6 shows the visual appearances of the histograms of the stego-images of Fig. 5.

Histogram also shows the maximum number of pixels having that same color. It is 37 in (a), 37 in (b), 99 in (c) and 99 in (d).

Table 6 shows the result of security analysis and robustness analysis, computed between Lana Color and Stego-Lena Color, with 81944 bits of hidden data and 114744 bits of hidden data in cover image.

Table 7 shows the result of security analysis and robustness analysis, computed between Pepper Color and Stego-Pepper Color, with 84336 bits of hidden data and 107008 bits of hidden.



(a)Histogram of Stego-Lena color with 81944 bits | **(b) Histogram of Stego-Lena color with 114744 Bits** | **(c) Histogram of Stego-Pepper color with 84336 bits** | **(d) Histogram of Pepper color with 107008 Bits**

Fig. 6. Histograms of Stego-color images

Table 6. Result of security and robustness analysis for the Lena color image

Method	81944 bits	114744 bits	Method	81944 bits	114744 bits
Jaccard	0.99999	0.99999	MSE	0.05198	0.0727
Intersection	0.99970	0.99958	PSNR	60.97379	59.5132
Correlation	0.99999	0.99998	UIQI	0.99998	0.99997
Chi-square	0.00029	0.00042	MSSIM	0.99998	0.99997
Bhattacharya	0.00099	0.00124			

Table 7. Result of security and robustness analysis for the Pepper color image

Method	84336 bits	107008 bits	Method	96064	107008 bits
Jaccard	0.99998	0.99997	MSE	0.18263	0.20546
Intersection	0.99843	0.99801	PSNR	55.51502	55.00346
Correlation	0.99993	0.99997	UIQI	0.99997	0.99996
Chi-square	0.00163	0.00206	MSSIM	0.99997	0.99996
Bhattacharya	0.00645	0.00693			

5 Conclusion

In this paper a method of image steganography is discussed. It is implemented for both the grayscale and color images. As this method does not use the least significant bit for insertion and retrieval process so message cannot be removed due to hardware imperfection and also cannot be altered by opponent. Experimental outcome be evidence for that the projected technique give good results for security analysis and robustness analysis and thus the projected technique provides the evidence to be strong and theoretically and practically it is very difficult to break this method. Due to these reasons this system is names as Secure and Robust Information Hiding Steganographic Scheme (SRIHSS).

Competing Interests

Author has declared that no competing interests exist.

References

[1] Juneja M, Sandhu PS. An analysis of LSB image steganography techniques in spatial domain. International Journal of Computer Science and Electronics Engineering (IJCSEE). 2013;1(2). ISSN 2320–401X (Print).

[2] Poornima R, Iswarya RJ. An overview of digital image steganography. International Journal of Computer Science & Engineering Survey. 2013;4(1).

[3] Morkel T, Eloff THP, Olivier MS. An overview of image steganography, ICSA research group, Department of Computer Science.

[4] Jammi Ashok, Raju Y, Munishankaralak S, Srinivas K, Jammi Ashok. steganography: An overview, et.01. International Journal of Engineering Science and Technology. 2010;2(10):5985-5992.

[5] Shikha Sharda, Sumit Budhiraja. Image steganography: A review. International Journal of Emerging Technology and Advance Engineering. 2013;3(1).

[6] Pavani M, Naganjaneyulu S, Nagaraju C. A survey on LSB based steganography methods. International Journal Of Engineering And Computer Science. 2013;2(8):2464-2467. ISSN:2319-7242.

[7] Johnson NF, Sushil Jajodia. Exploring steganography: Seeing the unseen, computer. IEEE.1998;31(2):26, 34. DOI: 10.1109/MC.1998.4655281.

[8] Ker, et al. Improves dection of LSB steganography in Grayscale Image, In Proc. 6th International Workshop, Toronto, Springer LNCS. 2004;3200:97-115.

[9] Khurrum Rahim Rashid, Aqsa Rashid, Nadeem Salamat, Saad Missen. Experimental analysis of matching technique of steganography for Greyscale and colour image. International Journal of Computer Science & Information Technology (IJCSIT). 2014;6(6).

[10] Jarno Mielikainen. LSB Matching Revisited, IEEE Signal Processing Letters; 2005.

[11] Potdar VM, Chang E. Grey level modification steganography for secret communication, 2nd IEEE International Conference on Industrial Informatics INDIN 2004, Berlin, Germany; 2004.

[12] Khurrum Rahim Rashid M, Nadeem Salamat, Saad Missen, Aqsa Rashid. Robust increased capacity image steganographic scheme. International Journal of Advanced Computer Science and Applications (IJACSA). 2014;5(11).

[13] Asha V, Nagabhushan P, Bhajantri NU. similarity measures for automatic defect detection on patterned textures. International Journal of Image Processing and Vision Sciences (IJIPVS). 2012;1(1).

[14] Rajkumar Yadav. Analysis of various image steganography techniques based upon PSNR metric. International Journal of P2P Network Trends and Technology. 2011;1(2). ISSN:2249-2615 .

[15] Ismail Avcibas, Bulent Sankur, Khalid Sayood. Statistical evaluation of image quality measure. Journal of Electronic Imaging. 2002;11(2):206-223.

[16] Zhou Wang, Hamid R. Sheikh. Image quality assessment: from error visibility to structural similarity. IEEE Transactions On Image Processing. 2004;13(4).

[17] Yousra A. Y. Al. Najjar, Soong DC. Comparison of image quality assessment: PSNR, HVS, UIQI, SSIM, IJSER. 2012;3(8). ISSN2229-5518.

[18] Amhamed Saffor, Abdul Rahman Ramli, Kwan-Hoong Ng. A comparative study of image compression between jpeg and wavelet. Malaysian Journal of Computer Science. 2001;14(1):39-45.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=934&id=6&aid=8128