ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 6 , June 2017

Application of Low Power Oscillator in Image Cryptosystem

Preethi B N, Veena H S

M. Tech, Department of ECE, BIT, Bengaluru
Associate Professor Department of ECE, BIT, Bengaluru

ABSTRACT: In the recent world, security is a prime important issue, and encryption is one of the best alternative way to ensure security. More over, there are many image encryption schemes have been proposed, each one of them has its own strength and weakness. This paper presents a new approach at improving the level of security and secrecy provided by the digital colour signal-based image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. This new proposed encryption algorithm can ensure the lossless of transmissions of images. In this Paper it shows the implementation of the random number generator by designing the low power oscillator to get in the image security, so that our main aim of the paper is to get image encryption in low power devices. This proposed idea is being studied and executed by getting good results. In this the existing and proposed system is compared for getting area is lesser than existing system. The salient features of the proposed image encryption method are loss-less, Symmetric key encryption, less very large number of secret keys, and key-dependent pixel value replacement

KEYWORDS*:* random number generator, Symmetric key encryption and decryption, low power oscillator

I.INTRODUCTION

In recent years, more and more consumer electronic services and devices, such as mobile phones and PDA (personal digital assistant), have also started to provide additional functions of saving and exchanging multimedia messages [10], [11]. The prevalence of multimedia technology in our society has promoted digital images and videos to play a more significant role than the traditional dull texts, which demands a serious protection of users' privacy. To fulfil such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties. Due to the tight relationship between chaos theory and cryptography, chaotic cryptography have been extended to design image and video encryption schemes .The simplest way to encrypt an image or a video is perhaps to consider the 2-D and 3-D stream as a 1-D data stream, and then encrypt this 1-D stream with any available key , such a simple idea of encryption is called naive encryption[7],. Although naive encryption is sufficient to protect digital images and videos in some civil applications, this issues have taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts.

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an enhanced image or to extract some useful information from it. It is a type of signal dispensation in which input is image, like video frame or photograph and output may be image or characteristics associated with that image. Usually Image Processing system includes treating images as two dimensional signals while applying already set signal processing methods to them. It is among rapidly growing technologies today, with its applications in various aspects of a business. Image Processing forms core research area within engineering and computer science disciplines too.

The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. This new proposed encryption algorithm can ensure the lossless of transmissions of images. In this Paper it shows the implementation of the random number generator by designing the low power oscillator to get in the image security, so that our main aim of the paper is to get image encryption in low power devices

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 6 , June 2017

II.BACKGROUND

Image encryption schemes have been increasingly studied to meet the demand for real –time secure image transmission over the internet and through wireless networks. Encryption is the process of transforming the information for its security
with the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over the various type of networks The security of digital image has become more and more important due to rapid evolution of the internet in the digital world today. The security of digital images has attracted more attention .
Following are the various goals of encryption/decryption which are commonly used for images.

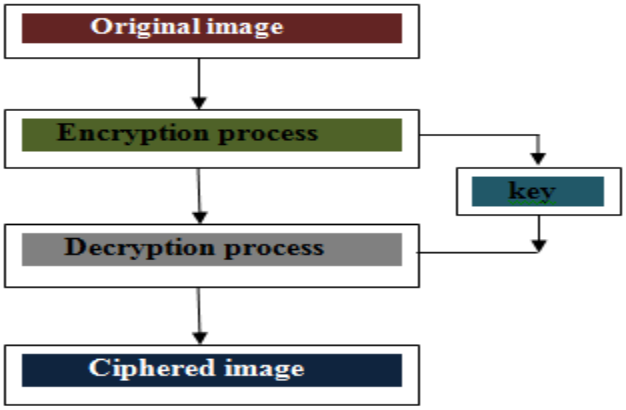
- **Confidentiality:** Information in the computer is transmitted and has to be accessed only by the authorized party.
- **Authentication:** The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.
- **Integrity:** Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- **Non Repudiation:** Ensures neither the sender, nor the receiver of message can deny the transmission.
- **Access Control:** Only the authorized parties are able to access the given information

There are two main categories of cryptography:

- **Secret key cryptography**
- **Public key cryptography**

- Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and receiver know the same secret code, called the key .Messages are encrypted by the sender using the key and ecrypted by receiver using the same key.
- Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data. The encryption/decryption process refers to the operation of dividing and replacing an arrangement of the original image .the image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transferred into new locations. For better process the block size should be small, because fewer pixels keep their neighbors. In this case the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side,
the original image can be obtained by the inverse transformation of the blocks. A general block diagram o this method is shown in figure below.



ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 6 , June 2017

III.PROPOSED METHOD

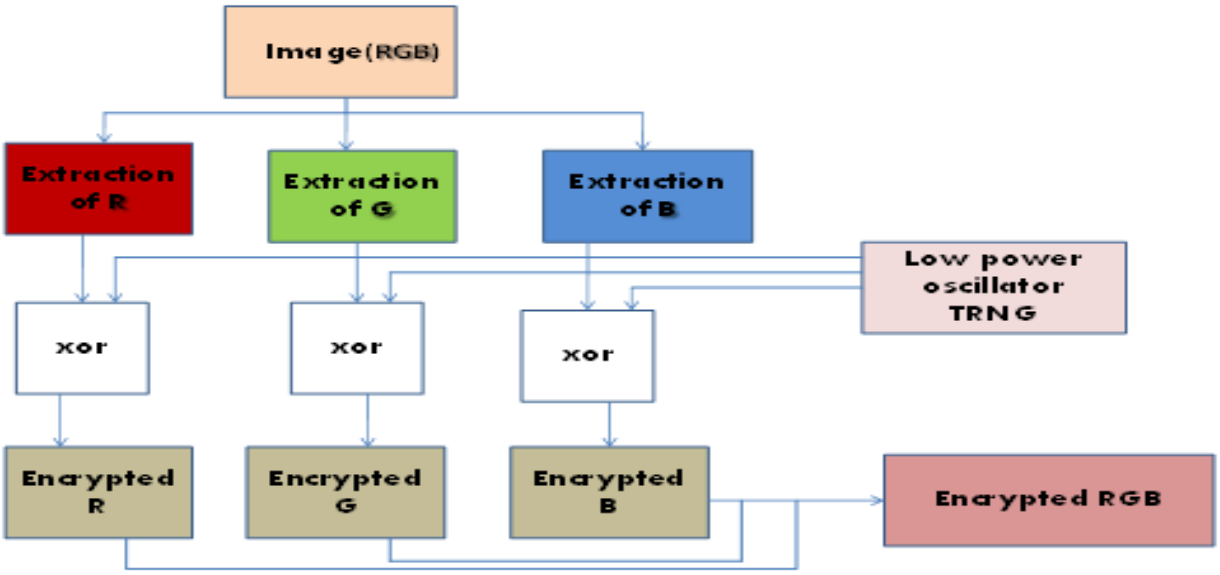


Fig. 2: proposed image Encryption Architecture

The original message is divided into a random number of blocks that are then shuffled within the image .The transformed image is represents individually as red, green and blue colored images. then fed to the xor operation with the TRNG from oscillator. The main idea is that an image can be viewed as an arrangement of blocks. Initially in proposed image encryption system requires .bmp or jpeg type of image file that is to be hidden. It has two modules encrypt and decrypt shown in figure. This module requires jpeg type of image message and gives the only one image file in destination. The decrypt module is used to get the hidden visual information in original image. It takes the cipher image file as an output and gives one file at destination folder, is that jpeg image file.

Below is the fig that represents the architecture for RNG generation in terms which acts as a key for encryption and decryption

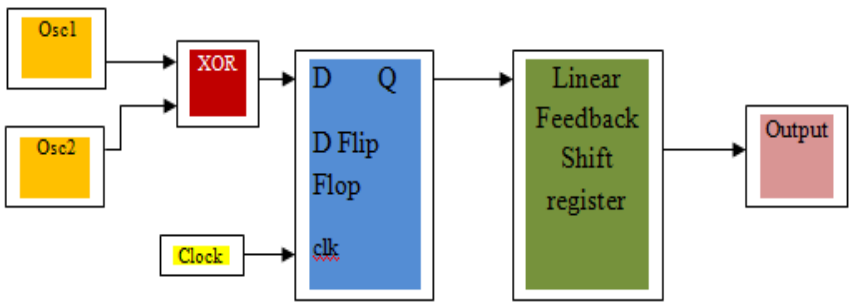


Fig. 3: Architecture of Proposed RNG

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 6 , June 2017

Fig. 3 depicts the architecture of the proposed TRNG [14], which consists of two oscillators named as OSC1 and OSC2, a low-power XOR gate and a D flip-flop. The outputs of OSC1 and OSC2 are combined by the XOR operation to yield Seed, a random sequence of higher statistical quality. The center frequencies of OSC1 and OSC2 are 62 and 48 MHz respectively so that the frequency of Seed are not integer multiple of half the clock frequency. The XOR operationis preferred owning to the even probability of 0s and 1s for Seed. Then Seed is sampled by a 5.4 MHz system clock usingthe D flip-flop. Post digital processor is added to further improve the randomness of the output random numbers.

The scheme of our post digital processor is shown in Fig. The proposed post digital processor is realized by 64bits Linear Feedback Shift Register (LFSR) and 4 non-linear combined functions, which can improve the unpredictability and de-correlation of output random sequence.

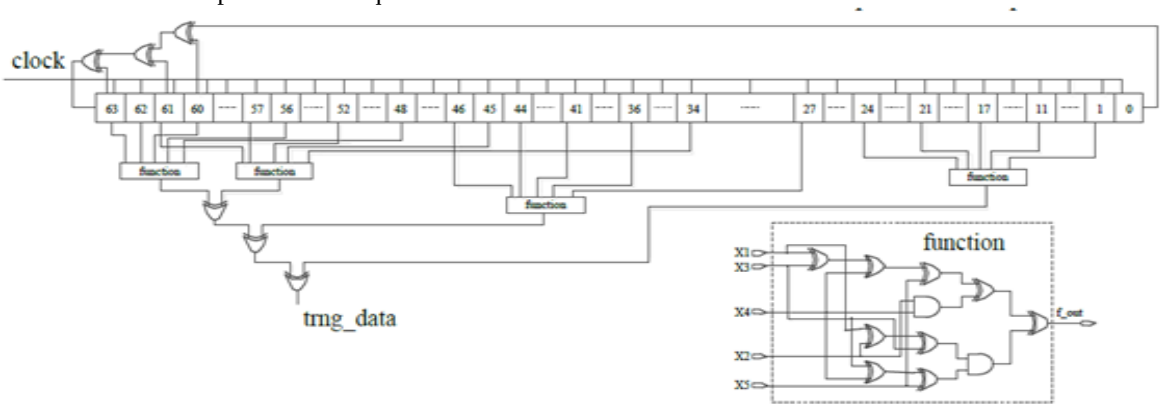


Fig. 4: Proposed Post Advanced Processor

IV.RESULT AND DISCUSSION

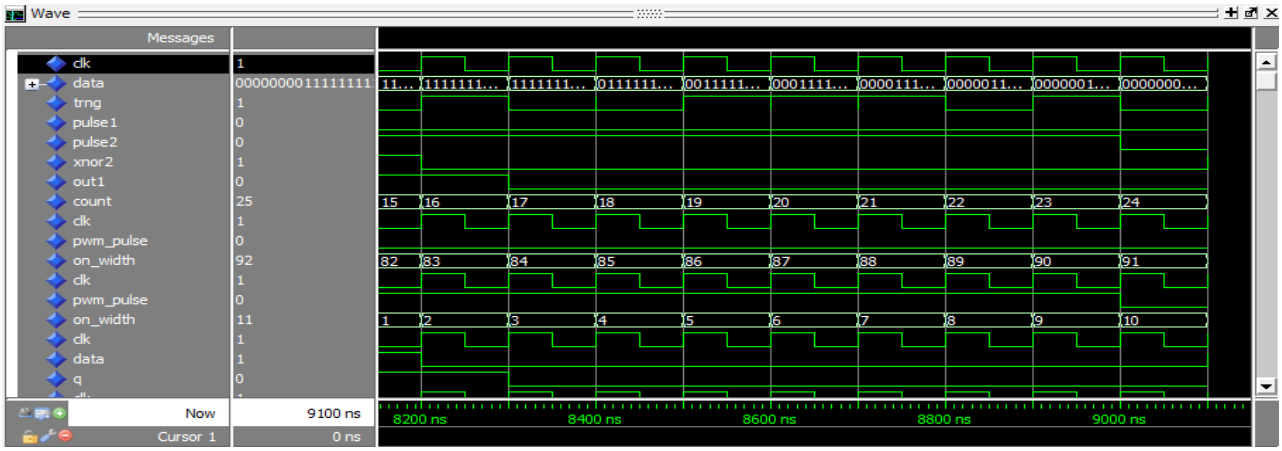


Fig. 5: Output sequence of proposed RNG

Above is the fig that represents the simulation result of proposed RNG which intern used as a key by both sender and receiver for encrypting and decrypting a true colour image respectively. Since the key is of RNG (Random number generator), it's become very difficult for an authorised user to crack what and which would be the key used for cryptography here.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 6 , June 2017

Below tables includes all the information about device utilisation, that is number of fliflop,LUTs etc used in the proposed and also the existing architecture for the key.

File Print E-mail Burn Open

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	126	768	16%
Number of Slice Flip Flops	85	1536	5%
Number of 4 input LUTs	209	1536	13%
Number of bonded IOBs	3	124	2%
Number of GCLKs	1	8	12%

Fig.6: Device utilization of proposed work

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	157	768	20%
Number of Slice Flip Flops	129	1536	8%
Number of 4 input LUTs	192	1536	12%
Number of bonded IOBs	66	124	53%
Number of GCLKs	1	8	12%

Fig.7: Device utilization of existing work

ENCRYPTION AND DECRYPTION

Fig.8: INPUT IMAGE

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 6 , June 2017

Below is the result that shows how image looks at each condition. Where figure 9 represents the extracted individual R (red) image from the original true colour image and the figure10 represents that the encrypted image of that extracted R, G and B of true colour image.

Fig. 9: Extraction of individual color from input image

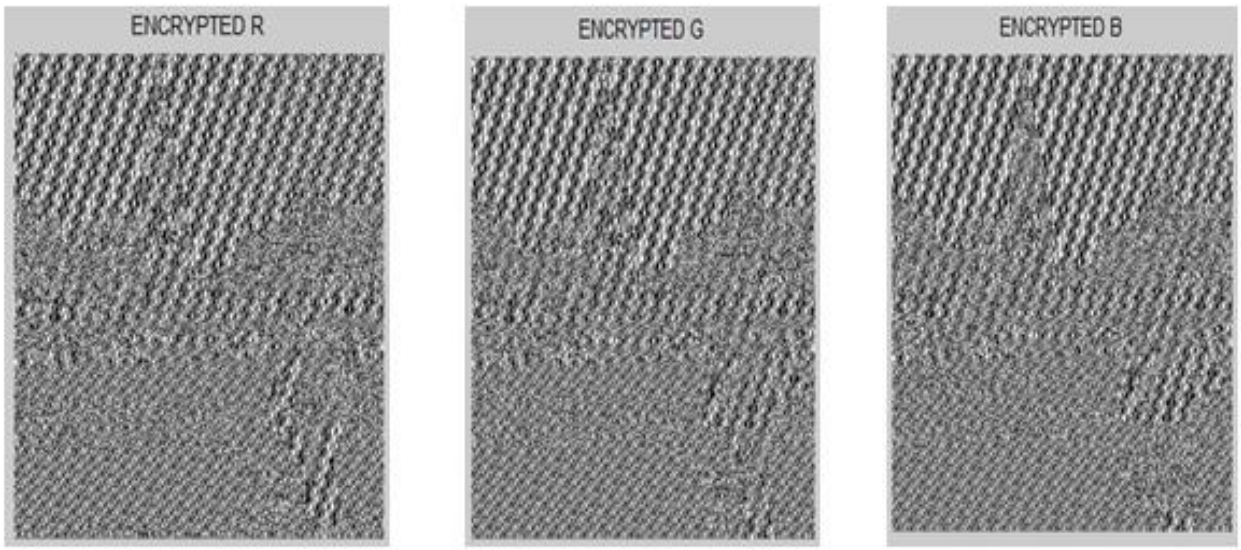


Fig. 10: Encrypted image of individuals extracted from input image

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 6 , June 2017

Below figures represents the overall image cryptosystem process

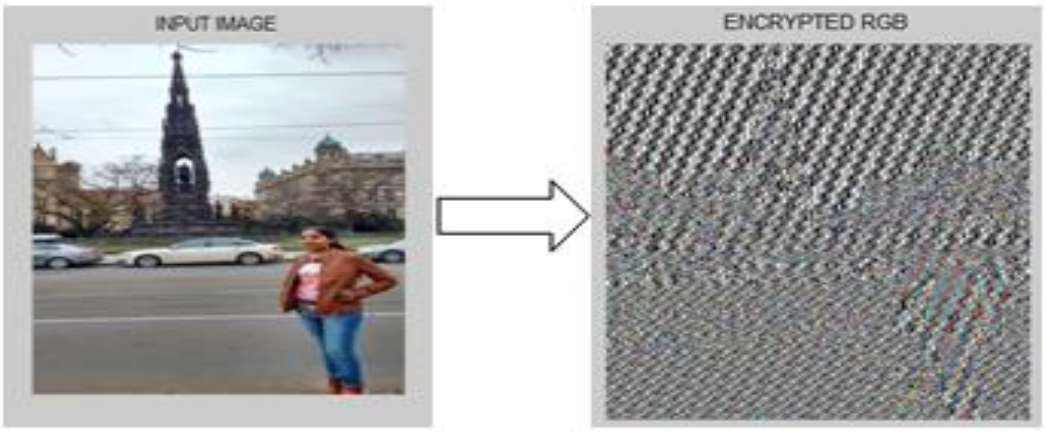


Fig. 11: Encryption of input image

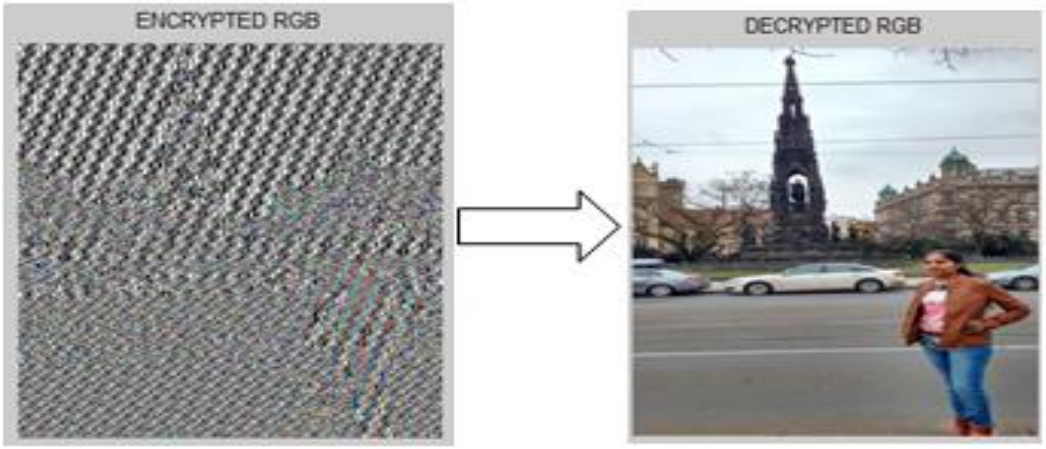


Fig. 12: Decryption of encryption image

V.CONCLUSION

The presents simulation results showed this approach has a better performance than other common encryption algorithms used. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance. This is because of the random key from the oscillator and the exor operation between that key and the extracted images of input image. Better key length will provide better symmetric algorithm implementation and security.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 6 , June 2017

REFERENCES

[1] L. Dongsheng ,L Zilong， L Lun*， Z Xuecheng , ―A Low-Cost Low-Power Ring Oscillator-based Truly Random Number Generator for Encryption on Smart Cards‖, IEEE Transactions on Circuits and Systems II: Express Briefs
[2] M. Bucci, L. Germani, R. Luzzi, A.Trifiletti, and M. Varanonuovo, ―A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC,‖ *IEEE Trans. Comput.*, vol.52, no.4, pp. 403-409, Apr. 2003.
[3] Harpreet Singh, Dr.Naveen Dhillon, Sukhpreet Singh Bains ―A New Approach For Image Cryptography Techniques‖, International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013
[4] G.A.Sathishkumar , Dr.K.Bhoopathy bagan and Dr.N.Sriraam ―Image Encryption Based On Diffusion And Multiple Chaotic Maps‖, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011
[5] Shujun Li, Xuan Zheng ―Cryptanalysis Of A Chaotic Image Encryption Method‖, 0-7803-7448- 7/02/$17 .*OO* 02002 IEEE
[6] Mohammad Ali Bani Younes and Arnan Jantan ―Image Encryption Using Block-Based Transformation Algorithm‖, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03
[7] Krishan Gupta ―Different Image Encryption And Decryption Techniques And Ka Image Cryptography‖, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106,
[8] K. Sakthidasan and B. V. Santhosh Krishna ―A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images‖, International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011
[9] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," *Int. J. of Reconfiugurable Computing*, vol. 2009, no. 4, pp. 1-8, Jan. 2009.
[10] A. Vassilev and T. A. Hall, "The importance of entropy to information security," *IEEE Trans.Comput.*, vol.47, no.2, pp. 78-81, Feb. 2014.
[11] B. Jun and P. Kocher, "The Intel RNG," White Paper, 1999 [Online]. Available: http://www.cryptography.com/intel RNG.pdf.
[12] B.S. Vikram and P.B. Wayne D. Golic, "Entropy and Energy Bounds for Metastability Based TRNG with Lightweight Post-Processing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 7, pp. 1785-1793, July 2015.