Journal of Engineering and Applied Sciences 13 (7): 1707-1712, 2018
ISSN: 1816-949X

A Novel Approach for Image Encryption Using M-J Set

[1]Yagyesh Godiyal, [2]Ashish Negi and [2]Deepak Negi
[1]Department of Computer Science and Applications,
Govind Ballabh Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand, India
[2]Department of Computer Science and Engineering,
Gyani Inder Singh Institute of Professional Studies, Uttarakhand, India

Abstract: The range and potency of the cryptography keys are vital attributes regarding encryption and decryption. The main objective is to achieve encryption of images with the help of chaotic encryption and fractal methods. The proposed algorithm is based on the fixed point and M-J set. The fixed point is generated by using iterative method of M-J set function. Random M-J set function can be used to generate fixed point. The fixed point generated is used as encryption key. The encryption methodology is fast but a bit lossy. The images are well encrypted and the keys used for encryption and decryption are robust enough to attain strong encryption. There is infinite no of M-J set functions can be used to generate encryption key, thus, providing extra layer of security for the users. Also, since, there is infinite no of Julia sets can be produced from different complex functions, the strength of key used for encryption is extensively increased. The proposed method is an effective method to achieve the encryption of images using fractals. It provides good level of encryption without affecting the quality of images too much. It is used for protection of images against various kinds of attacks.

Key words: Image encryption, chaotic encryption, fractal encryption, Mandelbrot set, Julia set, kinds

INTRODUCTION

Encryption is the soundest way to attain data security. The process of encryption secures the contents of a message and the original information is retrieved only through a decryption process. The aim of encryption is to prohibit illegitimate parties from viewing or modifying the data. Encryption is achieved by using some substitution technique, shifting technique, table references or mathematical operations. These processes generate a different form of data. The unencrypted data is referred to as the plaintext and the encrypted data is known as the cipher text.

The first researchers to explore and study the concepts of public key cryptology were (Stallings and Tahiliani, 2014; Stinson, 2005). Three most widely used public-key crypto-systems are RSA, Rabin and ElGamal. RSA system is named after its creators Rivest, Shamir and Adleman. RSA is based on the intractability of the integer factorization problem. The rabin cryptosystem was given by Buchmann (2004), Seberry and Pieprzyk (1989) and Menezes *et al*. (1996). It was the first asymmetric cryptosystem to describe the process of recovering the plaintext. The ElGamal encryption system was given by Buchmann (2004) and Seberry and Pieprzyk (1989). The ElGamal cryptosystem is applied in hybrid cryptosystem.

The theory, fractals is an active branch of nonlinear science. Fractal provide us the methods to relate with the self-similarity of objects and irregular phenomena in nature. For its suitable applications in many fields particularly in image processing, fractals have been accepted as a convinced technology in the world of cryptosystem. Euclidean geometry fails to explain some geometrical structures whereas fractal geometry can interpret with irregular geometric structures like cantor set, Koch curve, etc. (Mandelbrot, 1967, 1982). Fractal theory and its methodology provide people a new view and new idea which potentially be used in biometric cryptosystem and image encryption. The theory of fractals and fractal geometry gives rise to many new mysterious geometrical objects (Mandelbrot, 1982). So, the meaning of fractal and its actual application is exact opposite.

Fractals posse's infinite detail and generated by repeating patterns of same structure again and again. A fractal is never ending patterns and can have a highly complex structure. According to Mandelbrot (1982) classical Euclidean geometrical concepts were inappropriate at describing many natural objects such as clouds, mountains, coastlines and trees. Fractal geometry helps to clarify the concepts of these natural objects regarding their shape and geometry. The fractal geometry provides vital means to explain true geometry of nature as most of the concepts are directly related to natural

Corresponding Author: Yagyesh Godiyal, Department of Computer Science and Applications,
Govind Ballabh Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand, India

phenomenon. In fact, this new branch of mathematics strengthens the power of Euclidean geometry. Euclidean geometry interacts with objects in integer dimensions but fractal geometry interacts with non-integer dimension. This non-integer dimension is known as fractal dimension. Fractals are self-similar and independent of scale (Falconer, 2004; Peitgen and Richter, 2013).

Fractals have been gaining attention of various scientists and researchers and their applicability and popularity in various field of science is gaining momentum very rapidly. A large amount of research on chaos-based cryptosystems has been published. Much research has been done by incorporating chaotic maps into the design of symmetric and asymmetric encryption scheme. Kocarev and Tasev (2003) described a public key encryption method based on Chebyshev chaotic maps. Some research for incorporating of fractal functions into the design of symmetric and asymmetric encryption schemes using chaotic maps is given by Alia and Samsudin (2017).

Various methods and study have been already published in last decade explaining different image encryption algorithm based on M-J set. Al-Saidi and Rushdan (2009) presented a unique encryption method based on the theory of iterated function system. IFS is very important part in complex dynamic and fractal image compression. Sun *et al*. (2010, 2014) creates a random key by combining M-J set and the Hilbert transformation and improves Rozourvan's algorithm (Rozouvan, 2009). Lock *et al*. (2010) introduced a new approach of mixing image compression and encryption based on fractal geometric by converting Mandelbrot set and compressed image into square matrix and encrypting the image by using matrix operation. Agarwal and Negi (2014) following the study of Alia and Samsudin (2007a, b) proposed a key agreement protocol using superior mandelbrot set to calculate the public keys with the help of chosen private keys as input parameter whereas superior Julia set function is used to generate a shared private key by using public keys of either side for both parties using mann iteration.

Preliminaries: This study contains Diffie-Hellman cryptographic protocol, M-J set and their connection.

Diffie-Hellman cryptographic protocol: The purpose of the algorithm is to enable two users to transfer the secret key securely. Suppose, Aman (A) and Bilal (B) agree on a shared secret key using the Diffie-Hellman key agreement protocol (Stallings and Tahiliani, 2014; Stinson, 2005). The basic working of the protocol is shown in Fig. 1.

First, A produces a random private value a and B produces a random private value b. Both a and b are drawn from the set of integers. Then, Aman and Bilal

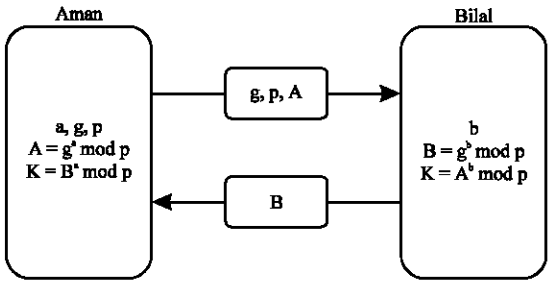

Fig. 1: Diffie-Hellmankey exchange

acquire their public values using parameters p and g and their private values. A 's public value is g a mod p and B's public value is g b mod p. They then swap their public values. Finally, A finds g ab = (g b) a mod p and B finds g ba = (g a) b mod p. Since, g ab = g ba = k, A and B now have a shared secret key k.

Mandelbrot and Julia set: Mandelbrot set and Julia sets are two most famous and crucial fractals in history of fractal geometry. In 1982, Benoit Mandelbrot began his refinement on Julia fractal set (Falconer, 2004; Peitgen and Richter, 2013).

Mandelbrot set is defined as the set of points on a complex plane generated by applying Eq. 2 iteratively. Although, Mandelbrot fractal set iterates with Z_0 starting at 0 and Julia set iterates starting with varying non-zero Z but actually they are both using the same basic fractal equation from Eq. 1 and 2. The connection between Mandelbrot fractal set and Julia fractal set is that each point c in the Mandelbrot is actually specifies the geometric structure of a corresponding Julia set (Mandelbrot, 1982; Falconer, 2004; Peitgen and Richter, 2013):

$$Z_n = z_{n-1}^2 + c;\ c,\ z_n \varepsilon\ C,\ n \varepsilon Z \quad (1)$$

$$Z_n = z_{n-1}^2 + c;\ z_0 = 0;\ c,\ z_{n-1} \varepsilon C,\ n \varepsilon Z \quad (2)$$

The Julia sets and their corresponding positions in Mandelbrot set is demonstrated in Fig. 2.

Proposed cryptographic protocol: Both sender and receiver will agree to use a same function in proposed cryptographic protocol. The following points are proposed on the basis of complex fractal functions. Both sender and receiver will agree to use same complex:

- Fractal function
- The fixed point which will be used for encryption of image is generated by the complex function used

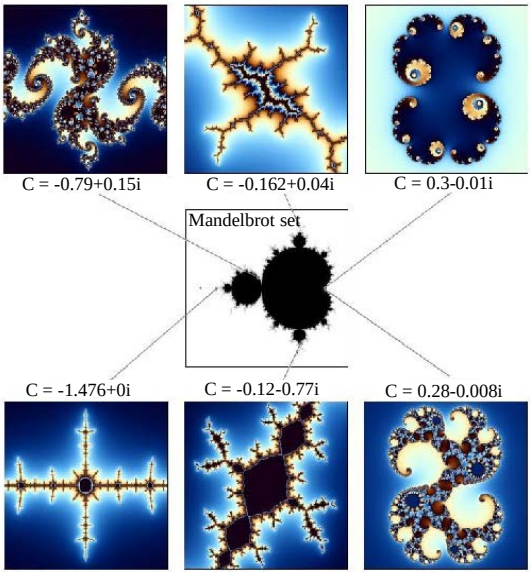

Fig. 2: Six Julia sets and their corresponding location in the Mandelbrot set

- Since, both sender and receiver had same function for generation of key (fixed point) based on their agreement they both have access to key
- The encrypted image was transferred to receiver
- The receiver finds the fixed point with the help of complex fractal function and decrypts the secure image
- The original image was obtained by decryption the encrypted image

One of the advantages of this scheme is that the complex fractal function is only known to sender and receiver. They can choose a function of their own choice and encrypt image using it. Every function generated a different fixed point, so, the choice for keys will be very large for a user.

MATERIALS AND METHODS

Proposed image encryption and decryption methodology: The proposed encryption and decryption scheme uses M-J set equations to operate and a function is used to generate a key which is used to achieve strong encryption. First of all a fixed point is calculated by using a complex function. This fixed point acts as private key for sender and receiver and is unknown to public. Since, it is up to sender to use any of function, so, it is not possible for some attacker to predict the type of function used by sender or user to encrypt and decrypt an image. The value of c (Eq. 1) acts as a public key and is known to sender

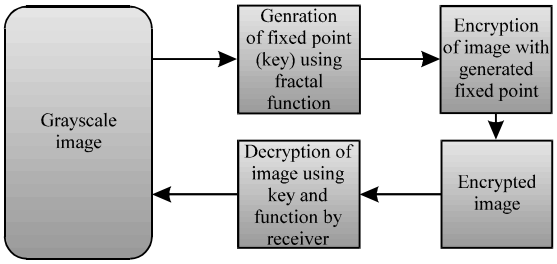

Fig. 3: Schematic diagram for proposed image encryption

and receiver from start. Even though if an attacker gets public key by some kind of cryptanalytic or brute force attack method the private key will be unknown to him and it is not possible for attacker exactly predict the exact same function used by sender and attacker and will not be able to get the decrypted image. The following proposed encryption and decryption scheme uses superimposition of fixed point's value over pixel values thus enabling strong encryption and an undetectable image. The image will only be decrypted by using correct function and correct public key making the proposed scheme very secure, efficient and effective. There can be infinite value of Julia sets enabling us a very large set of keys to choose from. The proposed algorithm for encryption and decryption is given:

- A grayscale image is used as an input
- A fixed point value is generated from a random complex function taken as per sender and receiver agreement
- The obtained fixed point is superimposed over image pixel values making image secure and encrypted
- The encrypted image is transferred from sender through a medium to receiver
- The receiver knows the fractal key and will used them on the encrypted image to get the original image or decrypted image
- The process will be stopped after the receiver gets the image

Figure 3 depicts the basic process to achieve encryption and decryption. The advantage of the proposed method is that it utilizes fractals to form the public and private keys for encryption and decryption the data. Further, the keys are generated at the sender and receiver end at runtime, therefore, increasing the level of security.

RESULTS AND DISCUSSION

The standard Lenna and Peppers image were used for encryption and decryption purposes. Both images are

grayscale in nature and have 256×256 resolution. The result obtained in MATLAB for encryption and decryption are shown in Fig. 4. The original, encrypted and decrypted images of Lenna are abbreviated as LO, LE

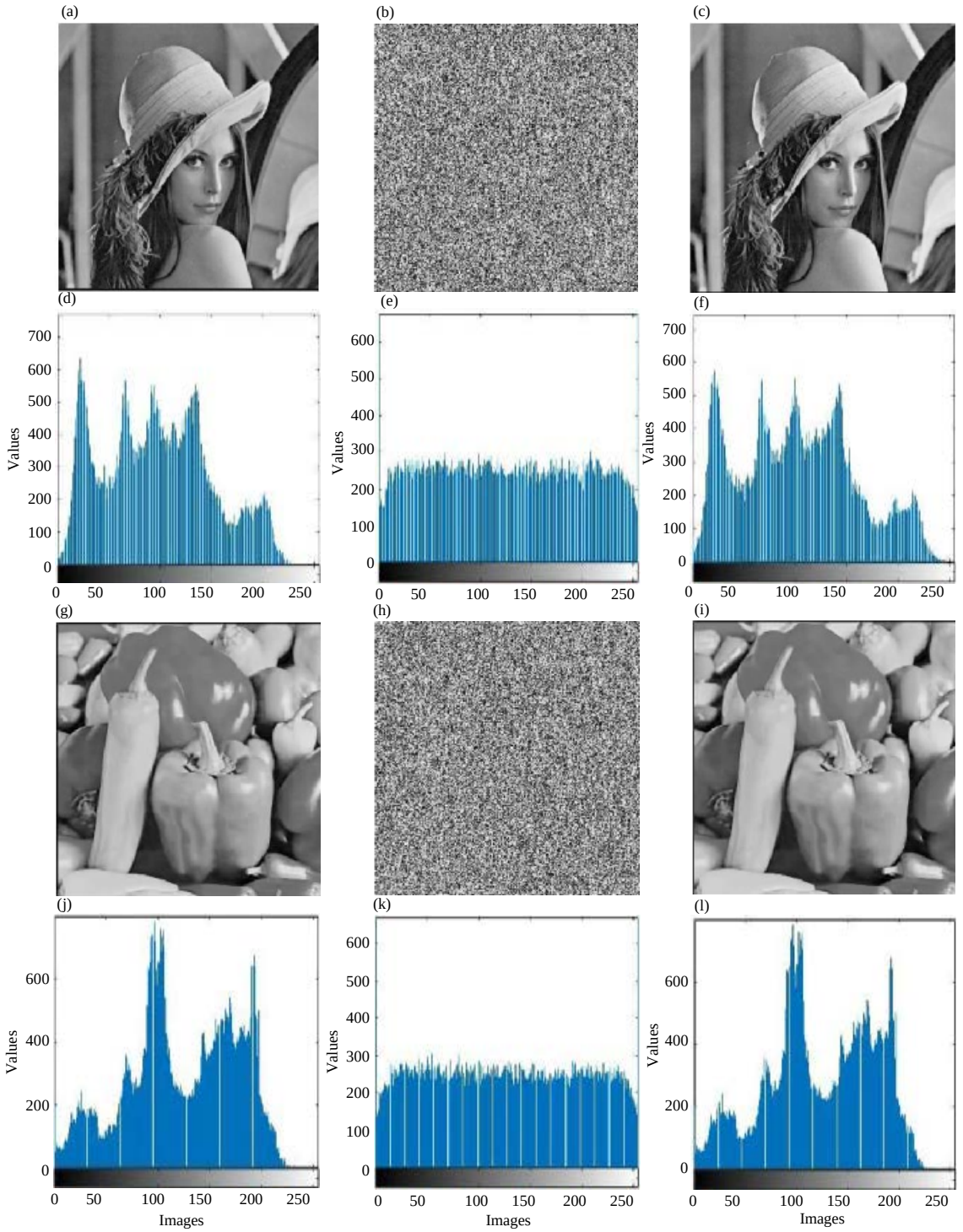

Fig. 4: Encryption results and histogram analysis of images: a) Original image (LO); b) Encrypted image (LE); c) Decrypted image (LD); d) Histogram of LO; e) Histogram of LE; f) Histogram of LD; g) Original image (PO); h) Encrypted image (PE); i) Decrypted image (PD); j) Histogram of PO; k) Histogram of PE and l) Histogram of PD

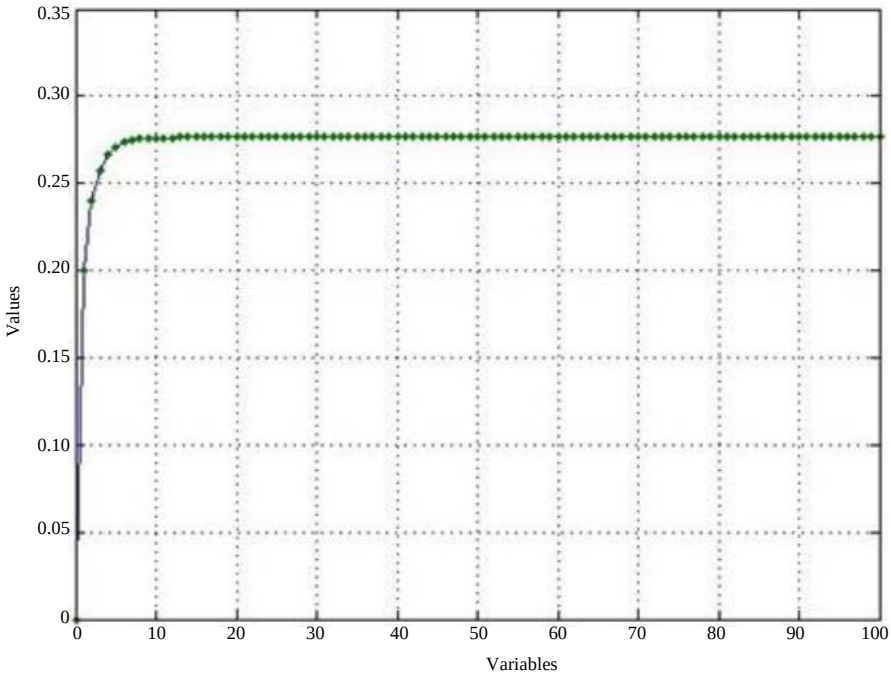

Fig. 5: Graphical representation of fixed point

Table 1: Tabular representation of fixed point generation

No. of iteration (n)	Corresponding fixed point
1	0.2000
5	0.2664
10	0.2759
15	0.2764
20-100	0.2764

and LD, respectively. The histogram analysis is also shown in Fig. 4. The results were encouraging and the encryption and decryption of image is fast. The decryption is a bit lossy. The function used here for the encryption and decryption is z (k+1) = z (k) 2+c. The function used can be changed according to the need of user, thus, providing extra security to the method. The graphical and tabular representation of fixed point generation and convergence are shown in Fig. 5 and Table 1. The histogram of encrypted images indicates the effectiveness of the incorporated methodology. Also, the method is secure as it's a type of chaotic encryption.

CONCLUSION

The encryption and decryption scheme is purely based on fractals. The encryption is strong and the encryption key is generated by random method, i.e. by iterating or by generating a fixed point. The method is suitable for encryption and decryption of grayscale images. The proposed method pro-vides good alternative for encryption of images. Further this method can also be applied to achieve text and sound encryption also.

REFERENCES

Agarwal, S. and A. Negi, 2014. A key agreement protocol based on superior fractal sets. J. Math. Comput. Sci., 4: 471-478.

Al-Saidi, N.M. and M.S. Rushdan, 2009. Using IFS as an encryption method. Proceedings of the International Conference on Education Technology and Computer (ICETC'09), April 17-20, 2009, IEEE, Singapore, ISBN:978-0-7695-3609-5, pp: 275-278.

Alia, M. and A. Samsudin, 2007b. A new public-key cryptosystem based on mandelbrot and julia fractal sets. Asian J. Inf. Technol., 6: 567-575.

Alia, M. and A. Samsudin, 2007a. New key exchange protocol based on Mandelbrot and Julia fractal sets. Intl. J. Comput. Sci. Netw. Secur., 7: 302-307.

Alia, M.A. and A.B. Samsudin, 2017. Generalized scheme for fractal based digital signature (GFDS). Intl. J. Comput. Sci. Netw. Secur., 7: 99-104.

Buchmann, J., 2004. Introduction to Cryptography. 2nd Edn., Springer, USA., ISBN: 978-0-387-21156-5, Pages: 335.

Falconer, K., 2004. Fractal Geometry: Mathematical Foundations and Applications. 2nd Edn., John Wiley and Sons, Hoboken, New Jersey, USA., Pages: 329.

Kocarev, L. and Z. Tasev, 2003. Public-key encryption based on Chebyshev maps. Proceedings of the 2003 International Symposium on Circuits and Systems (ISCAS'03) Vol. 3, May 25-28, 2003, IEEE, Bangkok, Thailand, pp: 3-3.

Lock, A.J.J., C.H. Loh, S.H. Juhari and A. Samsudin, 2010. Compression-encryption based on fractal geometric. Proceedings of the 2nd International Conference on Computer Research and Development, May 7-10, 2010, IEEE, Kuala Lumpur, Malaysia, ISBN:978-0-7695-4043-6, pp: 213-217.

Mandelbrot, B.B., 1967. How long is the coast of Britain? Statistical self-similarity and fractal dimension. Science, 156: 636-638.

Mandelbrot, B.B., 1982. The Fractal Geometry of Nature. W. H. Freeman and Company, ýNew York, USA., ISBN:9780716711865, Pages: 468.

Menezes, A.J., P.C.V. Oorschot and S.A. Vanstone, 1996. Handbook of Applied Cryptography. CRC Press, Boca Raton, USA., ISBN-13:978-0-84-938523-0, Pages: 755.

Peitgen, H.O. and P.H. Richter, 2013. The Beauty of Fractals: Images of Complex Dynamical Systems. Springer, Berlin, Germany, ISBN-13:978-3-642-61719-5, Pages: 197.

Rozouvan, V., 2009. Modulo image encryption with fractal keys. Opt. Lasers Eng., 47: 1-6.

Seberry, J. and J. Pieprzyk, 1989. Cryptography: An Introduction to Computer Security. 2nd Edn., Prentice-Hall, Inc., Upper Saddle River, New Jersey, USA., ISBN:9780724802746, Pages: 375.

Stallings, W. and M.P. Tahiliani, 2014. Cryptography and Network Security: Principles and Practice. Pearson, London, UK.,.

Stinson, D.R., 2005. Cryptography: Theory and Practice. 3rd Edn., CRC Press, Boca Raton, Florida, USA., ISBN:978-1-58488-508-5, Pages: 583.

Sun, Y., L. Chen, R. Xu and R. Kong, 2014. An image encryption algorithm utilizing Julia sets and Hilbert curves. PloS. One, 9: e84655-1-e84655-9.

Sun, Y.Y., R.Q. Kong, X.Y. Wang and L.C. Bi, 2010. An image encryption algorithm utilizing Mandelbrot set. Proceedings of the International Workshop on Chaos-Fractals Theories and Applications (IWCFTA'10), October 29-31, 2010, IEEE, Kunming, Yunnan, China, ISBN:978-1-4244-8815-5, pp: 170-173.