Evaluating the Performance and the Strength of CryptoBI Algorithm

Zakaria M. Abusilmiyeh [1], Tawfiq S. Barhoom [2]

[1]IT. Department, Islamic University of Gaza, Palestine

[2]IT. Department, Islamic University of Gaza, Palestine

***Abstract*—Cryptography problem is a key exchange between users securely, where no one else can obtain a copy. One proposed solution is CryptoBI "A Novel Cryptography Method Based on image for Key Generation" algorithm that prevents the attacks and avoids key exchanges between the two sides of communication by creating the key in home on the sender/receiver machine using RGB image. In this paper, we applied the CryptoBI algorithm and created a prototype for a specific scenario to measureits strength against the cryptanalysis, and to measure its efficiency against well-known symmetric cryptographic algorithms.The experiment results showed that the CryptoBI had higher data rate than AES, Rijndael, DES, 3DES, RC2 and RC6, but less than the Blowfish algorithm.In addition, the experiment results showed that the CryptoBI algorithm was weak against the cryptanalysis attack because it can be broken withinminutes when the CryptoBI images database is known to the attacker.**

Keywords*: Cryptography, Cryptanalysis, Cryptography key, Image key.*

I. INTRODUCTION

In the information age, sharing and transferring of data has increased tremendously and usually the information exchange is done using open channels which can make it vulnerable to interception. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts [1]. Cryptography is an important tool for protecting information. Cryptography presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination [2]. Many encryption algorithms are widely available and usedin information security. They can be categorizedin to Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption (e.g. RSA and ECC)[3]. Public key encryption is based on mathematical functions, computationally intensive and is not very efficient for small mobile devices[4][5][6]. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key. DES uses one 64-bits key. Triple DES(3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 is used various (128,192,256) bits keys [7][8][9][5][10][11][6][12]. The most common classification of encryption techniques can be shown in Figure 1.

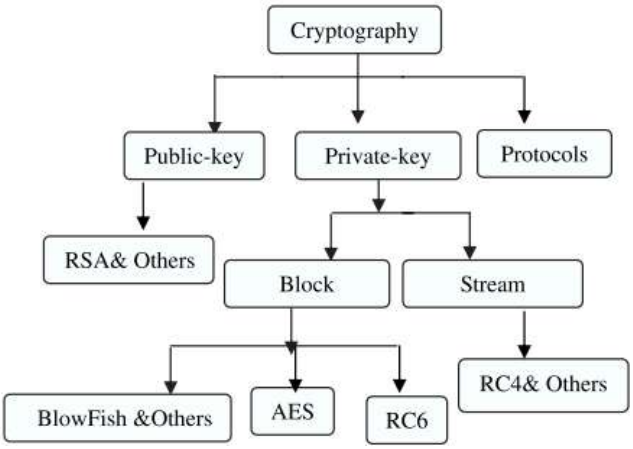

Figure 1: Overview of the field of cryptography[3].

Cryptography is considered to be one of the fundamental building blocks of computer security [13]. The key exchange is a method in cryptography by which cryptographic keys are exchanged between the sides of communication, allowing the use of a cryptographic algorithm[14]. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during the encryption and decryption separately.Thus, the concept of generating the key from an image came to the role [15].

The CryptoBI [16] is a new Cryptography method based on the key that is generated directly from an image stored in the database and the process of key generation based on sessions. The CryptoBI algorithm avoids key exchange between the two sides of communication and solves this issue efficiently by generating the key before starting the process of encryption

and decryption, rather than storing it.The most important characteristic of the CryptoBI that supports key-updating technique where the length of Key varies according to the size of the message, and it varies every session according to the session type.In this paper, we haveapplied the CryptoBI algorithm according to a specific scenario in order to measure itsstrength against the cryptanalysis and itsefficiency against well-known symmetric cryptographic algorithms, which are AES, Rijndael, DES, 3DES, RC2, RC6 and Blowfish.

The remaining parts of this paper are organized as follows: section 2 gives a short review of closely related literature. In section 3, we describe the details of an experimental design. In section 4, we provide and analyze the experimental results. In section 5, we conclude the paper.

II. LITERATURE REVIEW

Tamimi[17], provided a performance comparison between four most common algorithms: DES, 3DES, AES, and Blowfish. The comparison had been conducted by running several different settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. The simulation setup was in C# programming language. The results of this paper shows that blowfish has a better performance than other common encryption algorithms. AES showed poor performance results compared to other algorithms since it requires more processing power.Dhawan[18], has also done experiments for comparing the performance of the different encryption algorithms implemented inside .NET framework. Their results are close to the ones shown before. The comparison was performed on the following algorithms: DES, Triple DES (3DES), RC2 and AES (Rijndael).The results shows that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.Elminaamet. al.[3], presented a comparison of AES, DES, 3DES, RC2, Blowfish and RC6. They used different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. They concluded that in case of changing packet size Blowfish showed better performance than other algorithms followed by RC6. AES had better performance than RC2, DES, and 3DES. In case of changing key size it was concluded that higher key size leads to clear change in the battery and time consumption.

Singhal and Raina[19], presented a comparative analysis between AES and RC4 for better utilization. In this paper authors tried to find out performance comparison between block ciphers (AES) and stream cipher (RC4) algorithm. Based on the analysis and result, this paper concluded that which algorithm is better to use based on different performance metrics. The various metrics were: Encryption time, Decryption time, Throughput, CPU process time, Memory Utilization.

III. EXPERIMENTAL DESIGN

The evaluation of the CryptoBI algorithmis doneto measure: 1) **theperformance**, where the encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption; 2) t**he Strength,** we will use the cryptanalysis according to a specific scenario that can be used for this purpose. All algorithms have been implemented using C# programming language. We created a graphical user interface (GUI) application to simulate the performance of CryptoBI and to apply a compression with the performance of other symmetric cryptography algorithms.By using this application, we can transfer a text message or file between two points in LAN. We also created GUI interface to simulate the strength of CryptoBI against the cryptanalysis attack that tries to get plaintext from the ciphertext when the CryptoBI images database is known.This application implementation uses the provided classes in .NET environment to simulate the performance of AES, DES, 3DES, RC2 and Rijndael. Blowfish and RC6 implementation being used here is the one provided by Chilkat Software [Chilkat Encryption .NET Component] under the name of Crypt2[20].

For CryptoBI algorithm, we have created a database of color images which contains 24 images. The images are named as 1, 2…24 to specify the day hours because we used hourly session. We used red color image channel and K value equal to 8. The forms of simulation program used in the experiments are shown in figures 2, 3 and 4.The simulation program main form is shown below in Figure 2, which views the text messages and files that are received from the other host on the Local Area Network; the form accepts one input the cryptography algorithm.Figure 3 shows the sending form that is used to send the text messages or files to the other host. The form accepts four inputs: the recipient IP address, the recipient port, the cryptography algorithm, and the text or the file to send. Finally, Figure 4 shows the cryptanalysis form that is used to find the plaintext from the ciphertext. The form accepts as inputs an image from the database, the image channel, and the K value, which they are the synchronization setting of the CryptoBI algorithm.

The experiments conducted use LAPTOP: i5 2.30GHz with 4GB of RAM andThe simulation program is run inside the LAN environment.

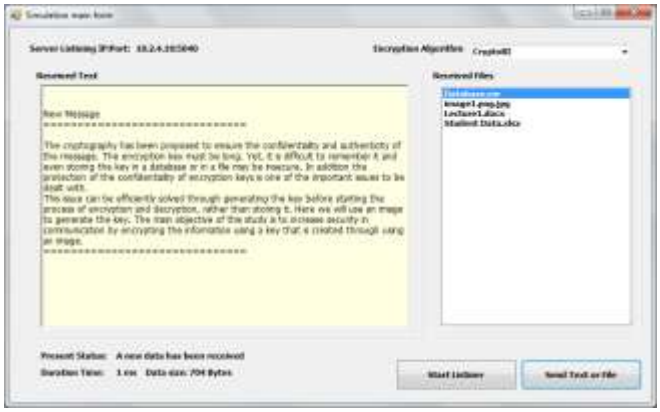

Figure 2: The main form of the simulation program, works as receiver.

Figure 3: The sending form of the simulation program

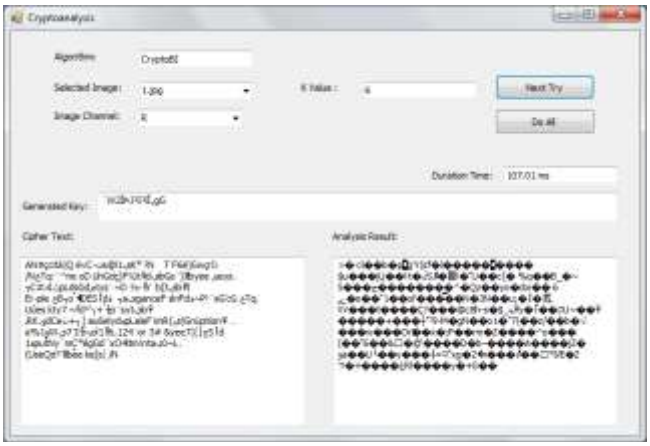

Figure 4: The CryptoBI Cryptanalysis form

In the experiments, the following tasks that will be performed are shown as follows:

- A comparison is conducted between the results of the selected different encryption schemes in terms of the encryption time.
- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.
- A study is performed on the effect of changing key size for cryptography CryptoBI algorithms on power consumption.
- A study is performed on the effect of cryptanalysis attack against the strength of CryptoBI.

IV. EXPERIMENTAL RESULTS

A. *Differentiate Output Results of Encryption Time*

Experimental results are given inFigure 5 for the encryption time comparison of CryptoBI with Blowfish, AES, DES, 3DES, RC2, RC6 and Rijndael using different data sizes ranging from 300 KB to 10 MB. We can realize that the curve of CryptoBI algorithm shows superiority over all algorithms except the Blowfish algorithm.

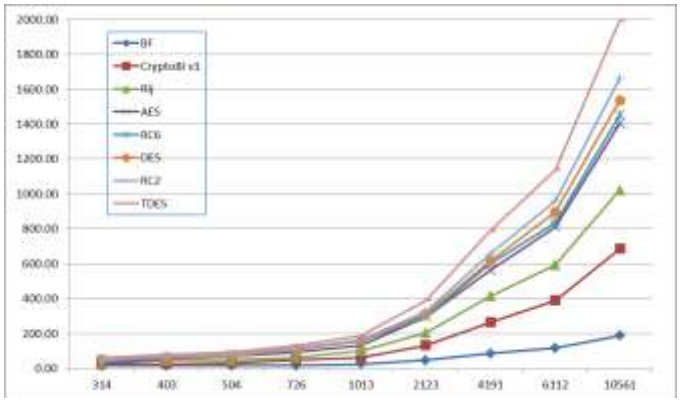

Figure 5: Time consumption of encryption algorithm.

B. *Effect of Changing Data Size for Cryptographic Algorithms on Power Consumption*

The encryption time is used to calculate the throughput of an encryption scheme. The throughput of the encryption scheme is calculated by equation 5[21]. The measured values of the average date rate for different algorithms are shown in table1. As the throughput value is increased, the power consumption of this encryption technique is decreased.

$$\text{Dravg} = \frac{1}{Nm}\sum_{i=1}^{Nm}\frac{Mi}{ti}\ (KB/s) \text{----------} (5)$$

Where:

• Dravg is the average data rate (KB /s).

• Nm is Number of messages or files with different sizes from 300KB to 10MB.

• Mi is the message or files size (KB).

• ti is the time taken to encrypt the message Mi .

Experimental results for this compassion point are shown in Figure 6 at the encryption stage. TheFigure 6 showed that the CryptoBI has higher data rate than AES, Rijndael, DES, 3DES, RC2, RC6, but less than the Blowfish

algorithm.Another point can be noticed here is that CryptoBIhas an advantage over other Rijndael, AES, RC6, DES, RC2 and TDES in terms of time consumption and throughput.

TABLE IV1: THROUGHPUT COMPARISON AT ENCRYPTION STAGE.

Encryption algorithm	Throughput or average data rate (KB /s)
Blowfish	42,847.72
CryptoBI v1	14,276.61
Rijndael	10,074.40
AES	7,693.41
RC6	6,864.29
DES	6,658.95
RC2	6,269.00
TDES	5,235.60

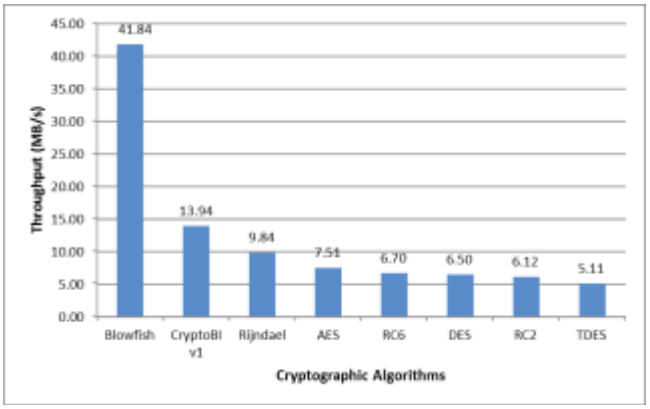

Figure 6: Throughput of each encryption algorithm (MB/Sec).

C. *The Effect of Changing Key Size of CryptoBI on Power Consumption*

The third performance comparison point is changing different key sizes for CryptoBIalgorithm. We consider the three different key sizes possible 128-bit, 256-bit and 512-bit keys. The Experimental results are shown in Figure 7.It can be seen that a higher key size does not lead to a clear change in the battery and time consumption.

D. *The Effect of Cryptanalysis Attack against the Strength of CryptoBI Algorithm*

The most difficult problem is presented when all that is available is the ciphertext only. In some cases, not even the encryption algorithm is known, but in general we can assume that the opponent does know the algorithm used for encryption. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. To break the CryptoBI algorithm we need to know the synchronization setting, which are images database, color image channel, K value and session type.

This experiment is performed under the following circumstances; having a ciphertext of a specific plaintext and having the images database, but the other synchronization settings are unknown, which are color image channel, the k value and the session type. These settings are necessary to get the cryptography key of ciphertext, so we have to guess the values of these unknown synchronization settings then run the key generation algorithm to produce the key which is used to decrypt the ciphertext. Then guess operation repeat until getting the plaintext from the ciphertext.

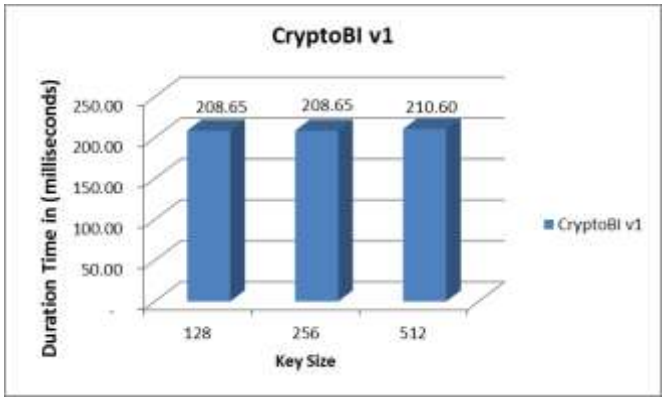

Figure 7: Time consumption for different key size.

The color image channel has three possible values R, G and B. The k value is between 0 and N, where N=$\sqrt{data\ length}$. Finally, the session time type determines the number of images in the database where there are 7 images for daily, 24 images for hourly or M images for custom session type. . Some of this experiment results are shown in table 2. The table shows the guessed values of the synchronization settings, the generated key using the guessed values, and the result of ciphertext decryption. After applying this scenario on the CryptoBI algorithm, the experimental result for CryptoBI algorithm is positive, and we get the key after 30 minutes of guessing the unknown synchronization settings, running the key generation algorithm, and running the decryption algorithm.

TABLE 2: SOME OF CRYPTANALYSIS RESULT FOR CRYPTOBI.

mage	Image Channel	K	Generated Key	Result (Success/ Fail)
1.JPG	R	1	jffjZfZ–UUšfªVf	Fail
1.JPG	R	6	jffjZfZ–UUšfªVfiª	Fail
1.JPG	R	7	jffjZfZ–UUšfªVfiªVª•	Fail
1.JPG	R	8	jffjZfZ–UUšfªVfiªVª•¦™–	Fail
1.JPG	R	9	jffjZfZ–UUšfªVfiªVª•¦™–e¦™	Fail

1.JPG	R	10	jffjZfZ–UUšfªVfiªVª•¦™–e¦™–jV	Fail
1.JPG	R	11	jffjZfZ–UUšfªVfiªVª•¦™–e¦™–jV¥UY	Fail
1.JPG	R	12	jffjZfZ–UUšfªVfiªVª•¦™–e¦™–jV¥UYf•e	Fail
3.JPG	R	4	¥Z©™™•YššifVVZšU	Fail
3.JPG	G	4	¦UU•¦iZf©fj¦Vš¥š	Fail
3.JPG	B	4	šjffjZfZ–UUšfªVf	Fail
3.JPG	R	8	¥Z©™™•YššifVVZšUišf–©fYY	Fail
5.JPG	R	8	jZeV¦i©Zf¦™ª••™Veff¦iš©e	Fail
5.JPG	R	16	eV¦Z–šiVijšeVšZVZ¥šªfe¥ViV¥Z™©VjY ZZejjU¥Uššie Vj	Fail
12.JPG	R	1	VieVf•™Ze¦Ve©fVU	Fail
12.JPG	R	2	VieVf•™Ze¦Ve©fVU	Fail
12.JPG	R	6	VieVf•™Ze¦Ve©fVUVe	Fail
12.JPG	R	7	VieVf•™Ze¦Ve©fVUVe¥iª	Fail
12.JPG	R	8	VieVf•™Ze¦Ve©fVUVe¥iª™YU	Success

V. CONCLUSION

The CryptoBI key is generated directly from an image which is selected from a database of images according to the session time, so the process of key generation is based on sessions. This approach is called the key-updating method which is a new approach to increase the difficulty to discover the key. To break this algorithm, we need to know the images database, color image channel, the k valueand the session type.This paper presents a performance evaluation of the CryptoBI algorithmand selected symmetric encryption algorithms which are AES, Rijndael, DES, 3DES, RC2, RC6 and Blowfish, as this paper presents an evaluation of the strength of CryptoBI algorithm against cryptanalysisaccording to a scenario.Several points can be concluded from the experimental results.

1. In case of changing packet size, it was concluded that CryptoBI had a better performance than the other symmetric encryption algorithms except the Blowfish.
2. In case of changing the key size of CryptoBI, it can be seen that higher key size doesn't lead to a change in the battery and time consumption.
3. Brute-force attack against the CryptoBI algorithmsby trying all possible keysbecomes impractical, because the CryptoBI generate large updating keys.
4. In case of cryptanalysis according to a scenario, where we assume that the attacker knows the algorithm and images database. It was concluded that the CryptoBI wasweak against the cryptanalysis.

The CryptoBI algorithm process has an advantage,that the key generation is based on a session.So in every session, we have a different key. As the key length varies according to data size, the key length can be more than 512 bits according to data size.

VI. THE FUTURE DIRECTIONS

Future scope for CryptoBI algorithm is that the key generation algorithm could be developed to improve the strengths of the key generation algorithm to generate random and unpredictable keys even if the images database is known. Finding a method to generate a key from image that is complicating the cryptanalysis work to break the algorithm by finding the cryptography key and make it impractical. Future work alsoisimproving the CryptoBI algorithm performance to be at the forefront ofotheralgorithms.

REFERENCES

[1] P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," Karur, India, 2010.

[2] W. Stallings, "Cryptography and Network Security - Principles and Practices", Pearson Education Third Edition ed., 2002.

[3] D. S. Abd Elminaam, H. M. Abdual Kader and M. M. Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms," *International Journal of Network Security*, Vols. Vol.10, No.3, p. 213–219, May 2010.

[4] *P. Ding, "Central manager: A solution to avoid denial of service attacks for wreless LANs," International Journal of Network Security, vol. 4, no. 1, pp. 35-44, 2007..*

[5] *Hardjono, Security In Wireless LANS And MANS, Artech House Publishers, 2005..*

[6] *P. Ruangchaijatupon, and P. Krishnamurthy, "Encryption and power consumption in wireless LANsN," The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28,2001..*

[7] *D. Coppersmith, "The data encryption standard(DES) and its strength against attacks," IBM Journal of Research and Development, pp. 243 -250, May1994..*

[8] *J.Daemen,and V.Rijmen,"Rijndael: Theadvanced encryption standard," Dr. Dobb's Journal, pp. 137139,*

Mar. 2001..

[9] *N. E. Fishawy, "Quality of encryption measurement of bitmap images with RC6, MRC6, and rijndael block cipher algorithms," International Journal of Network Security, pp. 241-251, Nov. 2007..*

[10] *M. S. Hwang and C. Y. Liu, "Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005..*

[11] *K. Naik, "Software implementation strategies for power-conscious systems," Mobile Networks and Applications,vol. 6, pp. 291-305, 2001..*

[12] *B. Schneier, The Blowfish Encryption Algorithm,Retrieved Oct. 25, 2008. (http://www.schneier.com/blowfish.html).*

[13] Seshadri, R. and T.RaghuTrivedi, "Efficient Cryptographic Key Generation using Biometrics," *Int. J. Comp. Tech. Appl.*, vol. 2 (1), pp. 183-187, 2011.

[14] "Wikipedia (Key exchange)," Dec. 1, 2013. [Online]. Available: (http://en.wikipedia.org/wiki/Key_exchange).

[15] Santhi, B., K.S. Ravichandran, A.P. Arun and L. Chakkarapani, "A Novel Cryptographic Key Generation Method Using Image Features," in *Research Journal of Information Technology 4(2)*, 2012.

[16] Barhoom, Tawfiq S. and Abusilmiyeh, Zakaria M., ""A Novel Cryptography Method Based on Image for Key Generation"," in *Palestinian International Conference on Information and Communication Technology*, Palestine, Gaza, 2013.

[17] *A. A. Tamimi, "Performance Analysis of Data Encryption Algorithms"*, Retrieved Oct. 1, 2008.

[18] *Dhawan, Priya; "Performance Comparison: Security Design Choices," Microsoft Developer Network October 2002. http://msdn2.microsoft.com/en-us/library/ms978415.aspx.*

[19] *Singhal, Nidhi and Raina, J P S. "Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology, ISSN: 2231-280, July to Aug Issue 2011, pp. 177-181..*

[20] "ChilKat Software," 2014. [Online]. Available: http://www.chilkatsoft.com/encryption-features.asp.

[21] G. R. a. R. UMARANI, *UMARAM: A NOVEL FAST ENCRYPTION ALGORITHM FOR DATA SECURITY IN LOCAL AREA NETWORK*, ICCCCT'10,IEEE, 2010.

[22] 2014. [Online]. Available: http://kb.bloombase.com/kb/?View=entry&EntryID=33.

[23] Asha A., Liyamol A. and Nisha V K, ""RC5 Encryption Using Key Derived From Fingerprint Image"," in *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference*, Dec. 2011.