A novel method for digital data encoding-decoding

Amjad Y. Hindi
Communication Engineering department, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan

Article Info

Article history:

Received Oct 6, 2019
Revised Feb 13, 2020
Accepted Feb 27, 2020

Keywords:

AES
Decoder
DES
Digital image
Encoder
Hight
Histogram
LED
Speedup

ABSTRACT

Cryptography is one of the paramount and most vital data treatment processes, it allows us to be secure in our electronic transactions. The process of cryptography protects our valuable data such as private account numbers and transaction amounts, electronic signatures replace handwritten signatures or credit card authorizations, and public-key encryption provides confidentiality. The objective of data encryption is to keep digital data confidentiality save as it is stored on computer systems and transferred using the internet or other computer networks. In this paper we will focus in enhancing security level of the encryption-decryption process by introducing a novel method, which uses any digital color image to encode-decode secret message, the using of a special key to encrypt-decrypt the encoded-decoded message, the color image will be known only by the transmitter and receiver to keep the process of data treatment confidential, the obtained experimental results by the proposed method will be analyzed to prove the enhancement in process efficiency and confidentiality.

Corresponding Author:

Amjad Y. Hindi,
Communication Engineering department,
Faculty of Engineering Technology,
Al-Balqa Applied University.
Email: amjadhindi@bau.edu.jo

1. INTRODUCTION

Digital color image [1-3] is one of most commonly used data types; it is usually represented by a 3D matrix (red, green, and blue colors are assigned to the first, second, and third dimensions correspondingly), each color value is ranges from 0 to 255, the repetition of each color value forms the image histogram [4, 5] as shown in Figures 1 and 2. If the color image is clear and normalized then the histogram will cover all the values between 0 and 255 [4, 5], thus the color values can be used to handle the ASCII value of any character in any secret message, allowing us to use the color image for secure data cryptography. The goal of data cryptography is to protect data and to improve the security wherever data is stored or conveyed [6]. Many methods were proposed to insure the security of transmitted secret message [7-9], which are using the techniques of data hiding, the secret message is to be hidden in a covering image, the covering image will be encrypted [10-15]. In this research, a new method which is falls in the category of standard method of data encryption-decryption such as DES, AES, LED, and hight methods.

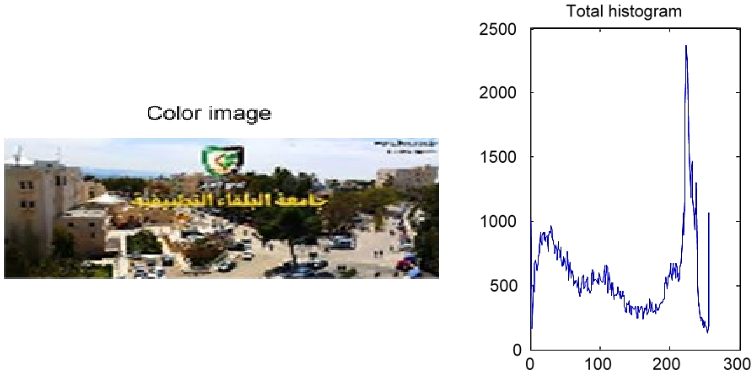

Figure 1. Color image and histogram

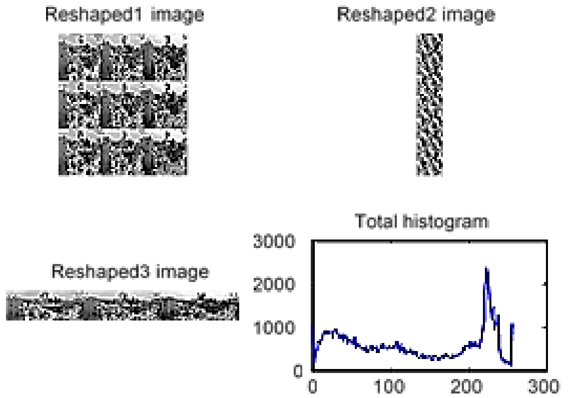

Figure 2. Reshaped color images and total histogram

2. BACKGROUND

2.1. DES encryption-decryption

Data encryption standard (DES) [16] is a block cipher, at the encryption site, DES divides the secret message into 64 bits blocks, takes a 64-bit text and makes a 64-bit code; at the receiving end, DES takes a 64-bit ciphertext and creates a 64-bit block. Theprocess of encryption is two parts which are initial permutationsand final permutations (P-boxes), and sixteen Feistel rounds [15, 17]. EachFeistel round uses a different key generated by an algorithm described below. Figure 3 shows the structure of data encryption standard at the sender site.

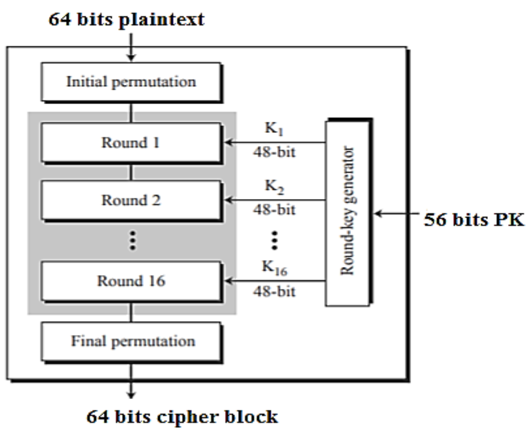

Figure 3. DES structure [18]

2.2. AES data encryption-decryption

Advanced encryption standard (AES) consists of two techniques for encryption and decryption of ciphertext. Which are known as substitution and permutation network (SPN) [19, 20]. AES dealswith plaintext blocks of 128 bits (16 bytes) size. Each block is represented by 4x4 matrixes and AES operates on a matrix of bytes. AES uses several rounds and logical-mathematical operation to perform encryption and decryption processes as shown in Figure 4 [20]

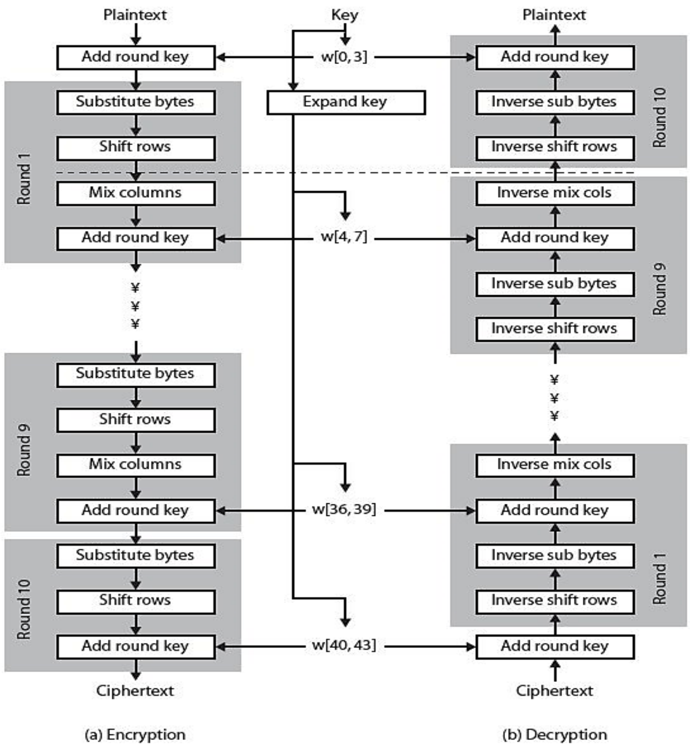

Figure 4. AES structure [15]

2.3. Hight data encryption-decreyption

HIGHT (High security and light weight) is a symmetric method of data encryption-decryption, which uses a 64 bit key and 64 bit ciphertext block and it is suitable for low-resource device [21]. Hight hasa simple structure with usesa basic arithmetic operation–XOR as shawn in Figure 5, addition/subtraction in modular 256, and circular shift rotation, without using S-Box [22, 23].

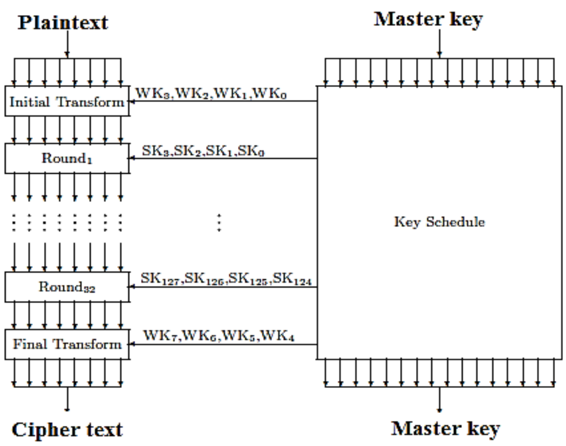

Figure 5. Hight structure [18]

2.4. LED data encryption-decryption

Light encryption device (LED) is an SPN type Lightweight block cipher was first introduced by Guo et al. in 2011 [24]. The step function performed 8 times for the 64 bit key and 12 times for the 128-bit keys. The keys used in LED block cipher may vary from 64 bits to 128 bits [25, 26]. LEDdivides the input key into two blocks of 64-bit keys and processesin parallel. So more than one input can be processed at a time, thereby the speed of architecture increased at the cost of the area. The operation involved in the architecture is add round key, add constant, substitute cells, shift rows and mix columns [26].

3. THE PROBLEM

Digital image has a huge size (the dimensions of a digital image are expressed in terms of its pixels, for instance "800x600" or "1520x1280" where the first number is the width of the photo and the second number the height of the photo). Using the available standards of data encryption-decryption for color images will require more efforts, the image must be divided into blocks, each block must be encrypted, and then decrypted. This will increase the encryption-decryption times, thus will decrease the standard methods efficiency.

4. THE PROPOSED SOLUTION

The proposed solution introduces a method that uses a digital color image to encode the secret message in the encrypption phase, and the same color image in the decryption phase as an image-decoder as shown in Figure 6. The following procedures show the implementation of the proposed method:

a) Encryption procedure:

Phase 1: Private key (PK) generation:

This phase will be implemented once by generating a random integer array with a big number of element to suit any message with any length, the generated PK must be saved and must be known by the sender and the reciever.

Phase 2: Message encoding:

Message encodinghas will be implemented as followes:

- Select the secret message.
- Get the length of the message.
- Select the image-encoder.
- Get the image size.
- Reshape the image into one row array.

For each character in the message find the first occuranes of character ASCII value in the image, and store the positing in encoded array.

Phase 3: Encryption phase:

The Encryption phase is performed by the following steps:

- Load PK
- Adjust the PK to match the message lengt.
- XOR the encoded array with PK to get the encrypted message.

Table 1 shows an example of message encryption.

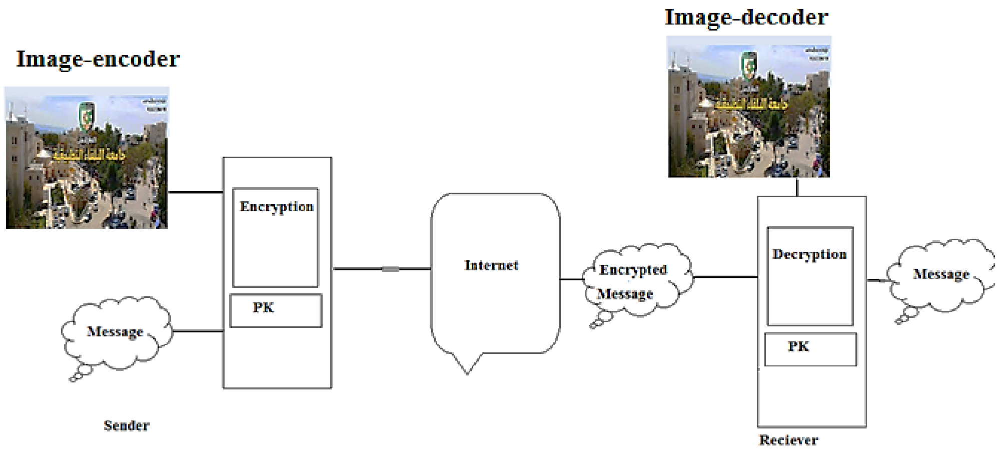

Figure 6. Proposed method structure

Table 1. Message encryption example

Message characters	Encoded message	Key	Encrypted message
z	1958	242	1876
i	1348	58	1406
a	1009	154	875
d	702	123	709
	1656	227	1691
a	1009	194	819
l	908	116	1016
q	2115	4	2119
a	1009	209	800
d	702	113	719
i	1348	156	1496

b) Decryption procedure:

Phase 1: Get PK:

By loading the PKthis phase can be implemented.

Phase 2: Get the decrypted message

The message treatement takes the following four steps:

- Use the encrypted message.
- find the message length.
- Adjust PK to suit the message length.
- XOR the key with the message to get the decoded message array.

Phase 3: Message decoding

The process of message decoding hasthe following steps:

- Get the decoded secret message.
- Get the length of the message.
- Select the image-decoder.
- Get the image size.
- Reshape the image into one row array.
- Use each value in the decoded message as a position in the image to get the pixel value as an ASCII code of the character.

5. IMPLEMENTATION AND EXPERIMENTAL RESULTS

A matlab code was writen to implement the proposed method of message encryption-decryption, several experiment were performed as followos:

a) Experiment 1: Encrypting the same secret message using various image-encoder:

One secret message was taken, the prposed method was implemented using various color images, Table 2 shows the results of this experiment. From the results shown in Table 2 we can see that using various color image as an encoders-decoders leads to producing different encoded and encrypted messages.

Table 2. Experiment 1 results

Original	Image 1		Image 2		Image 3		Image 4		Image 5	
message	Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted
z	2019	1809	133	119	159	109	403	353	132	118
i	61	7	243	201	260	318	487	477	79	117
a	76	214	222	68	311	429	384	282	73	211
d	33	90	224	155	270	373	1413	1534	75	48
	410	377	24	251	9946	9785	704	547	298	457
a	76	142	222	28	311	501	384	322	73	139
l	30	106	115	7	214	162	505	397	252	136
q	51	55	494	490	316	312	420	416	88	92
a	76	157	222	15	311	486	384	337	73	152
d	33	80	224	145	270	383	1413	1524	75	58
i	61	161	243	111	260	408	487	379	79	211

b) Experiment 2: Encrypting deffirent secret messages using the same image-encoder:

Different secret messages weres taken, the prposed method was implemented using the same color image as an encoder-decoder, Table 3 shows the results of this experiment. From the results shown in Table 3 we can see that using the same color image to encode-decode various messages leads to producing different encoded and encrypted messages.

Table 3. Experiment 2 results

Message 1		Message 2		Message 3		Message 4		Message 5	
Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted	Encoded	Encrypted
2019	1809	1271	1029	99	145	96	146	86	164
61	7	76	118	42	16	76	118	76	118
76	214	76	214	42	176	30	132	30	132
33	90	33	90	76	55	51	72	1421	1526
410	377	410	377	48	211	76	175	410	377
76	142	76	142	410	344	410	344	388	326
30	106	37	81	241	133	99	23	99	23
51	55	42	46	391	387	87	83	32	36
76	157	76	157	50	227	87	134	34	243
33	80	33	80	33	80	30	111	34	83
61	161	256	412	76	208	61	161	30	130

c) Experiment 3: Calculating encryption and decryption times

Different color images were selected as an encoder-decoder and used to encrypt-decrypt 8 bytes secret message, the results of this experiment are shown in Table 4. From the obtained results in this experiment we can see that any color image can be used as an encoder-decoder, but it is better to use an image with small size, this image will be suitable and will reduce the encryption time (encryption time includes encoding time and encryption time).

Table 4. Experiment 3 results

Image size	Encryption time(S)	Decryption time(S)
152x171x3	0.0390	0.00001
165x247x3	0.0420	0.00001
183x275x3	0.0490	0.00001
360x480x3	0.0660	0.00001
360x480x3	0.0710	0.00001
846x1504x3	0.2720	0.00001
981x1470x3	0.3090	0.00001
1071x1600x3	0.3570	0.00001

d) Experiment 4: Comparisons with other methods

A matlab codes were to implement other standards of message encryption-decryption, a message of 8 bytes length (64 bits block) was selected and treated by each method, Table 5 shows the results of this experiment. From the results shown in Table 5 we can see that the proposed method is the most efficient method, because it requires a minimum time for message encryption-decryption as shown in Figure 7.

Table 5. Experiment 4 results

Test	Proposed	DES	AES	LED	Hight
1	**0.0394**	0.0769	**0.3441**	0.3084	0.2663
2	**0.0393**	0.0763	**0.3448**	0.3089	0.2660
3	**0.0393**	0.0762	**0.3444**	0.3085	0.2667
4	**0.0394**	0.0769	**0.3449**	0.3088	0.2667
5	**0.0394**	0.0762	**0.3447**	0.3085	0.2670
6	**0.0396**	0.0766	**0.3447**	0.3085	0.2666
7	**0.0391**	0.0770	**0.3443**	0.3085	0.2664
8	**0.0390**	0.0767	**0.3442**	0.3084	0.2662
9	**0.0395**	0.0769	**0.3442**	0.3089	0.2666
10	**0.0399**	0.0760	**0.3442**	0.3080	0.2667

The average encryption times for the used methods were calculated, Table 6 shows the results of calculations. From the results shown in Table 6 we can calculate the speedup of the proposed method using the following formula:

$$Speedup = \frac{Othermethodtime}{Proposedmethodtime}$$

The results of speedup calculations are shown in Table 7. From the results shown in Table 7 we can see that the proposed method has a significant speedup comparing with other standards of data encryption.

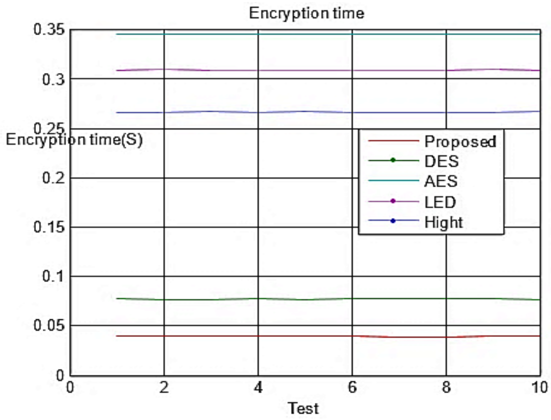

Figure 7. Time comparisons

Table 6. Average encryption time

Method	Encryption time(S)
DES	0.0760
AES	0.344000
LED	0.3080
Hight	0.266000
Proposed	0.0390

Table 7. Speedup calculation

Method	Speedup
DES	1.9487
AES	8.8205
LED	7.8974
Hight	6.8205

6. CONCLUSION

A novel method of data encryption-decryption based on image encoding-decoding was proposed, implemented and tested, from the obtained experimental results we can conclude that the proposed method has the following advantages compared with other standards used for data cryptography. Any digital image (color or gray) can be used as an encoder-decoder, any message can be encoded-decoded by any image, the same image can be used to encode-decode any message, the message length is unlimited, a message may be considered as one block, or it can be divided into block with various sizes. PK generation is a very simple process and it easy to update the key any time. The proposed method has a significant speedup, thus it is more efficient than other methods. The proposed method is very secure. It provides two level of security the PK level and encoder-decoder level.

REFERENCES

[1] Z. A. Alqadi, M. O. Al-Dwairi, A. A. Abu Jazar, R. A. Zneit, “Optimized True- RGB color Image Processing,” *World Applied Sciences Journal,* vol. 8, no. 10, pp. 1175-1182, 2010.
[2] Z. A. Alqadi, A. A. Moustafa, M. Alduari, “True Color Image Enhancement Using Morphological Operations,” *International Review on Computers & Software*, vol. 4, no. 5, pp. 557-562, 2009.
[3] A. Moustafa, Z. A. Alqadi, “Color Image Reconstruction Using A New R'G'I Model,” *Journal of Computer Science,* vol. 5, no. 4, pp. 250-254, 2009.

[4] J. A. Azzeh, H. Alhatamleh, Z. A. Alqadi, M. K. Abuzalata, "Creating a Color Map to be used to Convert a Gray Image to Color Image," *International Journal of Computer Applications,* vol. 153, no. 2, pp. 31-34, 2016.
[5] J. A. Azzeh, Z. Alqadi, M. Abuzalata, "Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 2, pp. 20-33, 2019.
[6] M. J. Aqel, Z. A. Alqadi, I. M. El Emary, "Analysis of Stream Cipher Security Algorithm," *Journal of Information and Computing Science,* vol. 2, no. 4, pp. 288-298, 2007.
[7] J. A. Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, M. Mesleh, "A Novel Based on Image Blocking Method to Encrypt-Decrypt Color," *International Journal on Informatics Visualization,* vol. 3, no. 1, pp 86-93, 2019.
[8] A. Y. Hindi, M. O. Dwairi, Z. A. AlQadi, "A Novel Technique for Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 9, no. 6, pp. 4942-4945, 2019.
[9] J. Nadir, Z. Alqadi, A. A. Ein, "Classification of Matrix Multiplication Methods Used to Encrypt-decrypt Color Image," *International Journal of Computer and Information Technology,* vol. 5, no. 5, pp. 459-464, 2016.
[10] M. J. Aqel, Z. A. Qadi, A. A. Abdullah, "RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication," *International Journal of Engineering & Technology,* vol. 7, no. 3.13, pp. 104-107, 2018.
[11] Z. A. Alqadi, M. O. Al-Dwairi, H. Zaini, et al., "ZJICD algorithm for JPEG image compression/decompression," *Elixir International Journal,* vol. 94, pp. 40368-40374*,* 2016.
[12] A. Y. Hendi, M. O. Dwairi, Z. A. Al-Qadi, and M. Soliman, "A Novel Simple and Highly Secure Method for Data Encryption-Decryption," *International Journal of Communication Networks and Information Security,* vol. 11, no. 1, pp. 232-238, 2019.
[13] J. Nadir, A. A. Ein , Z. Alqadi, "A Technique to Encrypt-decrypt Stereo Wave File," *International Journal of Computer and Information Technology*, vol. 05, no. 05, pp. 465-470, 2016.
[14] M. O. Al-Dwairi, A. Y. Hendi, M. S. Soliman, Z. A. A. Alqadi, "A new method for voice signal features creation," *International Journal of Electrical and Computer Engineering,* vol. 9, no. 5, pp. 4092~4098, 2019.
[15] M. O. Al-Dwairi, A. Y. Hendi, Z. A. AlQadi, "An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images," *Engineering, Technology & Applied Science Research,* vol. 9, no. 3, pp. 4165-4168, 2019.
[16] National Bureau of Standards NBS FIPS PUB 81, "Guidelines for Implementing and Using the NBS Data Encryption Standard, U.S. Department of Commerce," 1995.
[17] H. Alanazi, H. A. Jalab, A. A. Zaidan, B .B. Zaidan, "New Frame Work of Hidden Data with in Non Multimedia File," *International Journal of Computer and Network Security*, vol. 2, no. 1, pp. 46-54, 2010.
[18] A. W. Naji, S. A. Hameed, B. B. Zaidan, et al., "Novel Framework for Hidden Data in the Image Page within Executable File Using Computation between Advance Encryption Standard and Distortion Techniques," *International Journal of Computer Science and Information Security,* vol. 3, no. 1, pp. 73-78, 2009.
[19] Jain R., Jejurkar R., Chopade S., Vaidya S., & Sanap M., "AES Algorithm Using 512 Bit Key Implementation for Secure Communication," *International journal of innovative Research in Computer and Communication Engineering,* vol. 2, no. 3, pp. 3516-22, 2014.
[20] Abdullah A. M., Aziz R. H. H., "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *International Journal of Computer Applications,* vol. 143, no. 4, pp. 11-17, 2016.
[21] J. Daemen, L. Knudsen and V. Rijmen, "The Block Cipher Square," *International Workshop on Fast Software Encryption*, pp. 137-151, 1997.
[22] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication forRFID Systems Using the AES Algorithm," *International Workshop on Cryptographic Hardware and Embedded Systems,* 2004.
[23] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES Implementation on a Grain ofSand," *IEE Proceedings on Information Security*, vol. 152, no. 1, pp. 13-20, 2005.
[24] B. Jyrwa, R. Paily, "An Area-Throughput Efficient FPGA Implementation of Block Cipher AES Algorithm," *International Conference on Advances in computing, control, and telecommunication technologies,* 2009.
[25] Lim C. H., Korkishko T, "mCrypton – A Lightweight Block Cipher for Security of Low Cost RFID Tags and Sensors," *International Workshop on Information Security Applications*, 2005.
[26] Hong D., Sung J., Hong S., et al., "HIGHT: A New Block Cipher Suitable for Low-Resource Device," *8th International Workshop,* pp.46-59, 2006.