IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

# International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.317

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

# IoT-based Image Encryption: Analysis and Implementation Strategies

**Prof. Dr. Prateek Mishra**

Department of Electronics & Communication Engineering, Baderia Global Institute of Engineering & Management, Jabalpur (M.P.), India

**ABSTRACT:** With the proliferation of Internet of Things (IoT) devices, securing image data transmitted across diverse and often vulnerable networks has become a critical concern. This paper explores IoT-based image encryption methods, focusing on the analysis and implementation strategies to enhance data security in IoT environments. We begin by surveying existing encryption techniques and their suitability for IoT applications, highlighting the unique challenges posed by constrained devices, limited computational resources, and varying network conditions. Our analysis includes a comparison of traditional encryption algorithms with advanced cryptographic methods specifically adapted for IoT contexts. We then propose a novel image encryption framework tailored for IoT devices, emphasizing efficiency and scalability. This framework integrates lightweight encryption algorithms and adaptive key management strategies to balance security and performance. Experimental results demonstrate the effectiveness of our approach in terms of encryption strength, computational overhead, and energy consumption. The findings offer valuable insights into optimizing image encryption for IoT systems, contributing to the development of more secure and efficient IoT-based image transmission solutions.

**KEYWORDS:** IoT;Security; Encryption; Wireless Sensor Network, WSN;

## I. INTRODUCTION

An important issue in digital transmission and storage is Security and it can be provided by image encryption. The ways to provide high security when images are transmitted over the network is encryption. Image encryption changes the pixels of the image and decrease the correlation between pixels. Several different Image encryption techniques to protect confidential image data from unauthorized access are available which provide transmission of digital images in secure way. Algorithms which are good for textual data, may not be suitable for multimedia data because images contain large data. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code while they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. Mostly images are used in today's world to represent information in domains varying from corporate world, health care, document organization, military operations etc.Image encryption techniques convert original image into image that is hard to detect called cipher image. Decryption is the reverse process of encryption in which cipher image is converted into original image by providing the key which is used in encryption.Information is transmitted over the internet in which it is easy to disclose important information from theft so encryption techniques are being used. Encryption is basically used to protect secret information from unauthorized access. The image data have special properties such as bulk capability, high redundancy and high correlation in the pixels.

### Cryptography

There are many schemes used for enciphering which constitute the area of study known as cryptography.

### 1.1 Types of Cryptography

There are two main types of cryptography:
1) Secret key cryptography
2) Public key cryptography

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

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

Cryptography which can be used when secret messages are transferred from one party to another, Cryptography needs algorithm for encryption of data.

**1.2 Techniques for Encryption and Decryption**

Computer networks have been widely applied, people's communications have had a revolutionary change, and transmission of digital images over the internet has become more and more popular. The openness and sharing of networks exposes the security of digital images to threats in the process of transmission. People have to pay more and more attention to security and confidentiality of multimedia information. In various protection methods, the image encryption technique is one of the most efficient and common methods for the protection of image information. Traditional encryption algorithms, like Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES), etc., are not good for image encryption. So a new research method of image encryption is acquired urgently. The chaotic system is a deterministic nonlinear system. It possesses varied characteristics, like high sensitivity to initial conditions, determinacy and so on. Chaotic sequences which can be produced by chaotic maps are pseudo-random sequences; their structures are complex and difficult to analyze and predict. Chaotic systems can improve the security of encryption systems. The extant cryptography algorithms based on chaotic maps can be classified into two kinds: permutation and diffusion. In permutation stage, the positions of pixels from the original image are changed by chaotic sequences or by some matrix transformation. The permutation algorithm has a better encryption effect, but without changing its pixel values, leading to the histogram of the encryption image and the original image being duplicates; thus its security could be threatened the statistical analysis. In diffusion stage, the pixel values of the original image are changed by chaotic sequences. These methods are directly implemented encryption by overlaying a chaotic sequence generated by a single chaotic map and the pixel grey value from the image. If compared to the permutation, diffusion may lead to higher security, but the encryption effect is not good, in order to improve the security and the encryption effect, some researchers have combined permutation and diffusion. An image encryption algorithm based on one dimensional chaotic map. However, a single chaotic map used to encrypt image may lead to a smaller key space and lower security, so some new ways to develop efficient image-encryption schemes have been suggested. The experiment on DNA computing, initiated a new stage in the information age. In subsequent research, the characteristics of DNA computing, massive parallelism, huge storage and ultra-low power consumption had been found. The research on DNA computing, DNA cryptography emerged as a new cryptographic field, in which DNA is used as an information carrier and modern biological technology is used as implementation tool presented an image encryption algorithm of one-time pad cryptography with DNA strands. They pointed out that current practical applications of cryptographic systems based on one-time pads are limited to the confines of conventional electronic media. But DNA has extraordinary information density and is very suitable to store a huge one-time pad. Their method might be effective for solving the storage problem of the one-time pad. Various successfully hid the famous ‘‘June 6 invasion: Normandy’’ in DNA microdots. A novel encoding method is alternative to traditional binary encoding. Nucleotides are used as a quaternary code and each letter is denoted by three nucleotides. For example, use CGA to denote the letter A use CCA to denote the letter B, etc. Then, the secret message is encoded into a DNA sequence for example, AB is expressed as CCGCCA. For the two DNA cryptography schemes described above, biological experiments have to be done in the encryption and decryption steps. These experiments can be done in a well equipped lab using current technology, and it is very costly. For these reasons, the research on DNA cryptography is much more theoretical than practical. A pseudo DNA cryptography method, which has better encryption and was not through real biological experiments, it was only used to encrypt character information. In order to overcome the above shortcomings from image encryption based on chaotic maps and DNA cryptography, in this we use the simple theory of the DNA sequence operation to encrypt image information and the combined chaotic maps and DNA sequence addition operation to implement image encryption. DNA encoding and decoding for image A DNA sequence contains four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, and G and C are complementary. In binary, 0 and 1 are complementary, so 00 and 11 are complementary, 01 and 10 are also complementary. In this, we use C, A, T, G to denote 00, 01, 10, 11, respectively. For 8 bit grey images, each pixel can be expressed a DNA sequence whose length is 4. For example: If the first pixel value of the original image is 173, convert it into a binary stream as [10101101], by using the above DNA encoding rule to encode the stream, we can get a DNA sequence [TTGA]. Using 00, 01, 10, 11 to denote C, A, T, G, respectively, to decode the above DNA sequence, we can get a binary sequence [10101101].

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

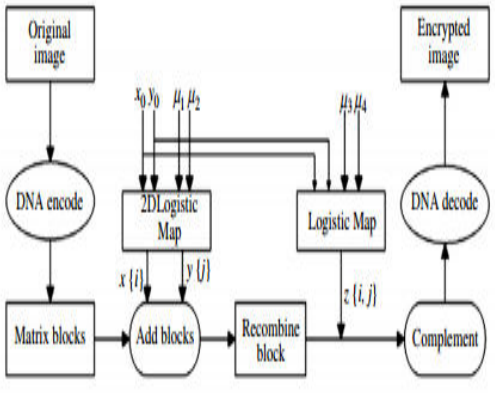



Figure1: Block diagram for DNA based image encryption algorithm.

## II. PROBLEM FORMULATION

In DNA encryption the execution time for image encryption is higher and memory utilization increases on number of round discussed in previous work. In proposed work, efforts are made to reduce the execution time and memory utilization for secure image encryption.

### 2.1.Motivation

An attack can be performed by sensing the communication in two nodes which is known as a man-in-the-middle attack. No reliable solution has been proposed in previous works to cater such attacks. Encryption could lead to minimize the amount of damage done to the data integrity. To assure data unification while it is stored in the middle ware and also during the transmission it is necessary to have a security mechanism. Algorithms have been developed that addresses the said matter, their utilization in IoT is questionable as the hardware we deal in the IoT are not suitable for the implementation of computationally expensive encryption algorithms. This Algorithm is designed for IoT to deal with the security and resource utilization challenges mentioned.

### 2.2.Objective

The main objective is to reduce the execution time and memory utilization to achieve fast image encryption. This methodology for Encryption could lead to minimize the amount of damage done to the data integrity.
To improve the correlation coefficient between the encrypted and decrypted image and win against statistical attacks to make it suitable to be integrated on IoT platform.Complex algorithm, however, may compromise the desired integrity. The objective is to overcome these problems.

## III. SIMULATION SETUP AND MATLAB

In this chapter, we are discussing about the software package platform and simulation tool utilized in the simulations. Chosen simulation parameter and also the varied metrics thought-about within the performance analysis of the proposed scheme. Finally, we'll discuss about the performance metrics used within the comparisons.

### 3.1 The Platform

All the simulation, implementation and analysis work is done on Windows 10. Since the platform provided the premise for doing everything, so it becomes essential to debate some options and additionally somewhat on however it evolved and the way it actively operating behind the scenes.

## IV. RESULT AND DISCUSSION

### 4.1 Technique Overview

The increased number of communication is expected to generate mountains of data and the security of data can be a threat. The devices in the architecture are smaller in size and low powered. Conventional encryption algorithms are computationally expensive due to their complexity and require many rounds to encrypt, wasting the constrained energy of the gadgets. Complex algorithm, however, may compromise the desired integrity. In this we propose an encryption

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

algorithm named as IOT image encryption. It's a 64-bit block cipher and requires 64-bit key to encrypt the data. The architecture of the algorithm is a mixture of feistel and a uniform substitution-permutation network. Simulations result shows the algorithm provides security in just five encryption rounds. The hardware implementation of the algorithm can be done on a low cost 8-bit micro-controller and the results of code size, memory utilization and encryption/decryption execution cycles are compared with benchmark encryption algorithms. The MATLAB code for simulations is available. The Internet of Things (IoT) is turning out to be an emerging discussion in the field of research and practical implementation in the recent years. IoT is a model that includes ordinary entities with the capability to sense and communicate with devices using Internet. As the broadband Internet is accessible and its cost of connectivity is also reduced, more gadgets and sensors are getting connected to it. conditions are providing suitable ground for the growth of IoT. There is great deal of complexities around the IoT, since we wish to approach object from anywhere in the world. The chips and sensors are embedded in the physical things that surround us, each transmitting valuable data. The process of sharing large amount of data begins with the devices themselves which must securely communicate with the IoT platform. This platform integrates the data from many devices and applies analytics to share the valuable data with the applications. The IoT is taking the conventional internet, sensor network and mobile network to next level as everything will be connected to the internet. A matter of concern that must be kept under consideration is to ensure the issues related to confidentiality, data integrity and authenticity that will emerge on account of security and privacy.

### 4.2 Methodology

The image encryption starts with input image. Lena.jpg image has been used as an input image to understand the performance of proposed work and previous work. Input image is selected through MATLAB by executing encryption program written on the editor window and a security key is assigned to input image encryption to make it more secure. Strong key selection is important for efficient encryption of image, Performance of encryption is determined by obtaining entropy and correlation coefficient of the image. The higher the entropy (meaning the more ways the system can be arranged), the more the system is disordered. This is used to encrypt image on adding more randomness to make image not possible to detect.

**High Entropy Mean Highly Secured Encryption**

These results are compared with the previous results to evaluate the performance of proposed work.Performance parameter can be understood by below description

#### 4.2.1 Evaluation Parameters

To test the security strength of the proposed algorithm, the algorithm is evaluated on the basis of the following criterion. Key sensitivity, effect of cipher on the entropy, correlation of the image. We further tested the algorithm for computational resource utilization and computational complexity. For this we observe the memory utilization and total computational time utilized by the algorithm for the key generation, encryption and decryption.

### 4.3 SIMULATION AND RESULTS.

Our result analysis is based on parameters mentioned below;

Performance of IOT encryption is determined by obtaining **entropy** and **correlationCoefficient** of the image.

**Correlation Coefficient Analysis**

The correlation between two vertically as well as horizontally adjacent pixels in the original image and its encrypted image has also been analyzed. Correlation is a statistical measurement of the relationship between two variables which ranges from +1 to - 1. As it is well known that in any image the correlation of adjacent pixels is very high, i.e. a good encryption algorithm is required to lower the correlation between adjacent pixels.

(a1 a2 a3 a4), (b1 b2 c3 d4) areCorrelation Coefficient of key metrics formula.

### 4.4 ALGORITHM

Step1.Key Expansion for five rounds

Step2.After the generation of round keys, encryption process can be started.

Step3.check execution time.

Step4. Check Memory Utilization.

Step5. Measure the amount of information in terms of entropy,

Step6. Calculate the correlation coefficient for original and encrypted images.

Step7. comparisons of results.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

## FLOW CHART OF METHODOLOGY

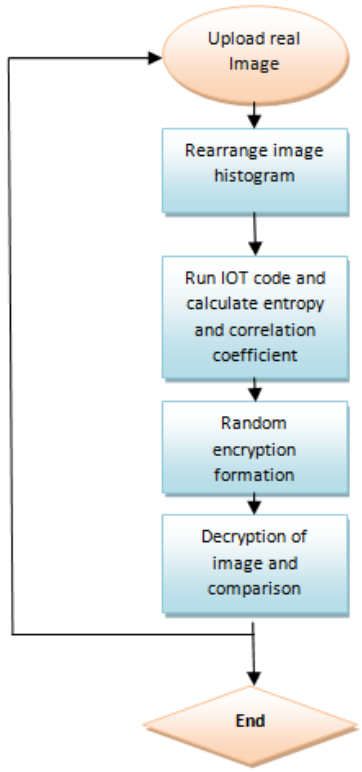



Figure 1.1: Flow Chart of proposed Methodology

## MATLAB RESULTS

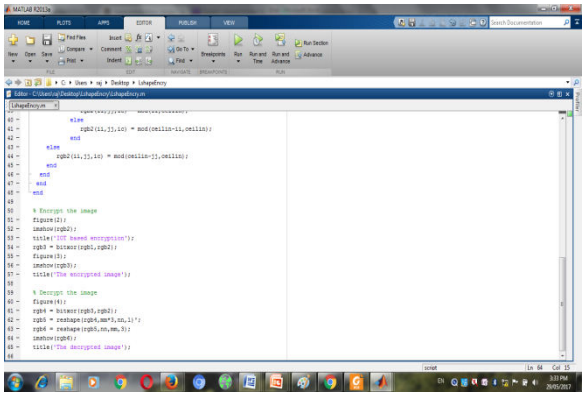


Figure 1.2:Matlab code

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

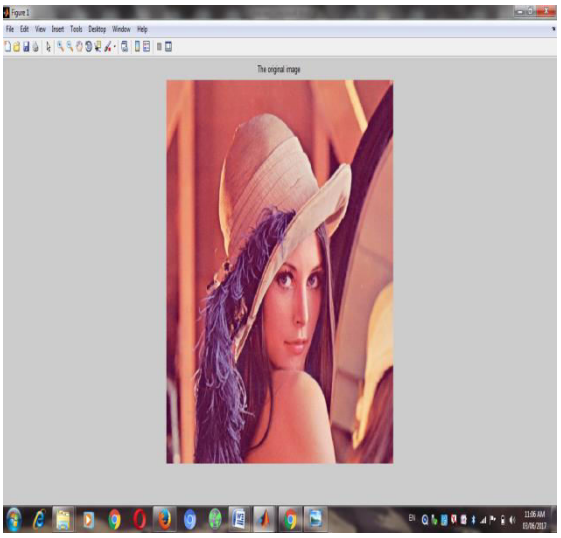


Figure 1.3: Input image for encryption

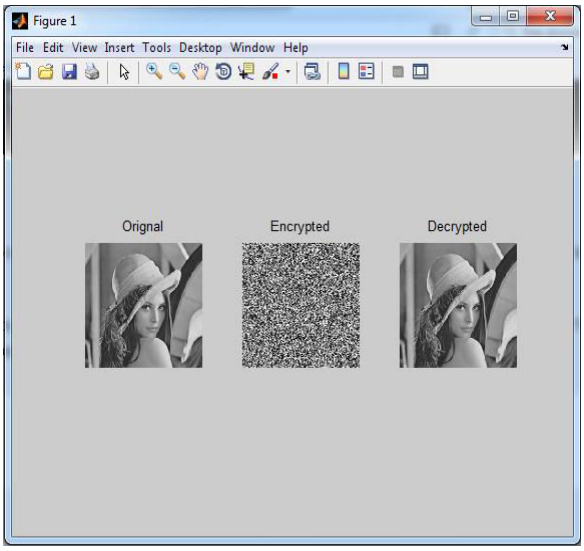



Figure 1.3: (a) Input image for encryption for Entropy Calculation

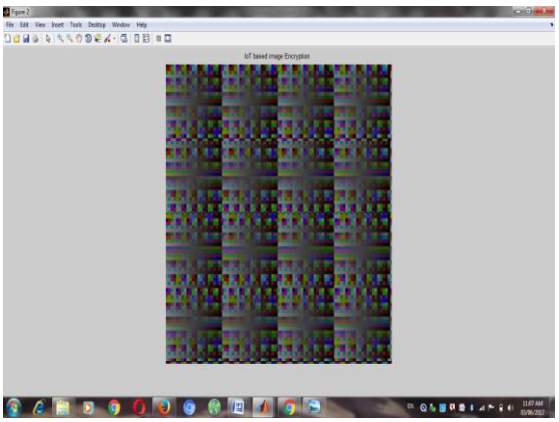


Figure 1.4: (a) IoT based image encryption

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

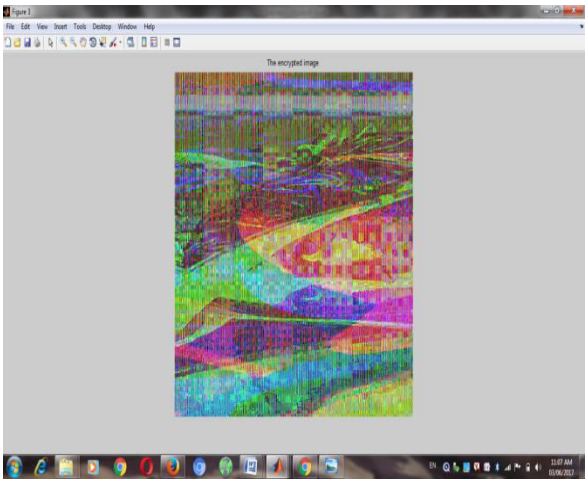


Figure 1.4: (b) encrypted image

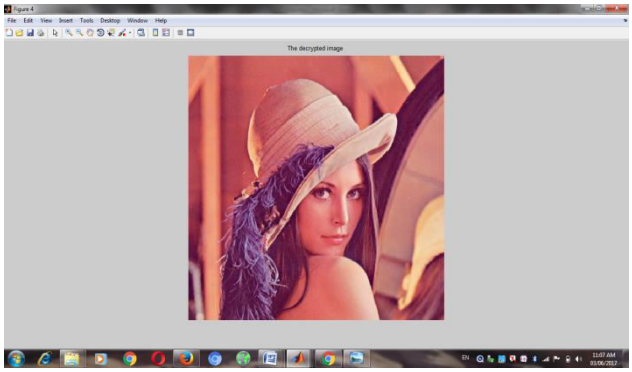


Figure 1.5 output decrypted image

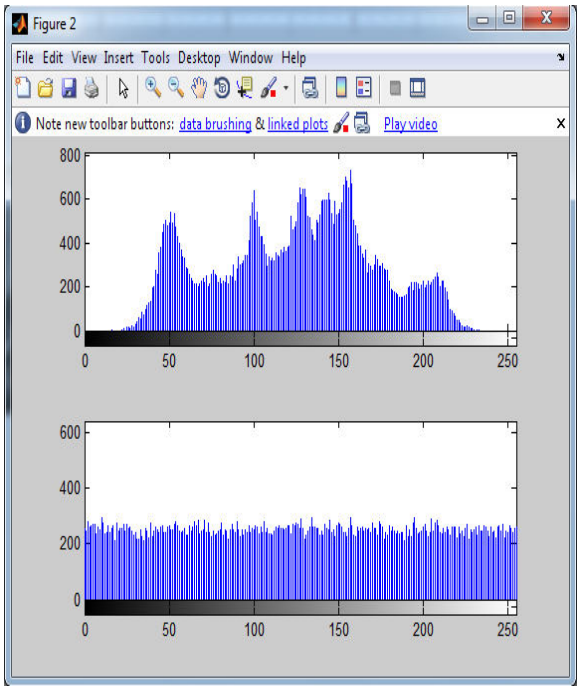



Figure 1.6: Output

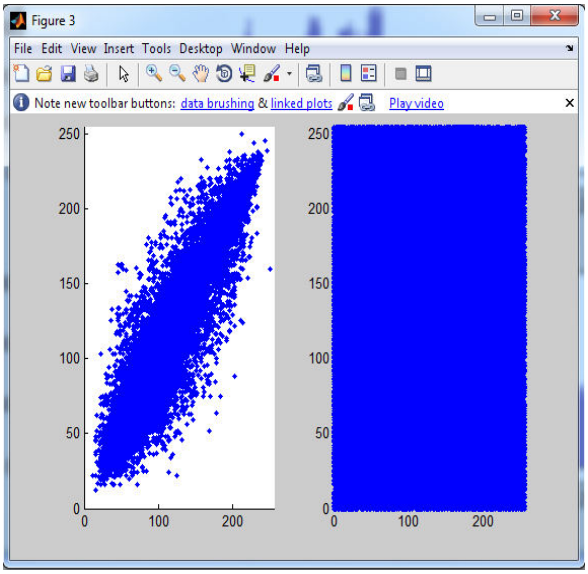
| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

Whereas; the below figure shows graphical representation of input image of size 256 x 256 and above plot shows variation in the input image(256x256) pixels after encryption which exceeds upto (0-800) in the X-axis & (0-256) in Y-axis.

Image intense pixal parts are defined for original input image and image has been assigned same intensity histogram for encryption so that it can not be detected.




(a) (b)

Figure 4.7: Corelation Calculation

Where figure (b) shows the plot of input image of size 256 x 256 and figure (a)shows the plot of encrypted image. The blue part in (a) represents its correlation with (b) i.e. up to what extent they are attainable to statistical attacks. Lower the correlation coefficient (lesser the similarity of (a) & (b))better the performance.

Corelation coofficient of image size 0-200 and 0-250 compares similar part of image with original image showing least correlation among the pixels.

### 4.5 RESULT COMPARISON

An encryption algorithm discussed in base paper[1] is composed of several computational rounds that may occupy significant memory making it unsuitable to be utilized in IoT. Therefore; the proposed algorithm is evaluated in terms of its memory utilization the proposed algorithm utilizes the 22 bytes of memory. The software environment is MATLAB2014a, the hardware environment is win10 system, the processor is i3, the RAM is 4GB, and thehard disk is PC with 500G. With the above simulation environment, simulation and analysis are carried out for thesecret key, the entropy of information, the anti-differential ability, and the ability against statistical attack.

**Result comparison Table**

| Parameter selection | DNA encryption | IoT encryption (proposed methodology) |
|---|---|---|
| Entropy | 7.9979 | 7.9983 |
| Correlation | 0.0152(High) | 0.0040 (low) |
| Memory cost | Cost High | Low cost |

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

Re is showing the Entropy for lena. Proposed work based on IOT has five rounds of calculation which makes proposed method better than DNA based image Encryption. And Total encryption time: 29.933036.
DNA encryption gets the entropy of information: 7.9979 which is close to IoT based entropy around 7.9983 but memory cost and run time consume more than IoT.

## V. CONCLUSION

The communication is expected to generatedata and the security of data can be a threat. Thedevices in the architecture are smaller in size and low powered. Old encryption algorithms are generallycomputationally expensive due to their complexity and requiresmany rounds to encrypt, essentially wasting the constrained energy of the gadgets. Less complex algorithm,Simulationsresult shows the algorithm provides substantial security in justfive encryption rounds. The hardware implementation of the algorithm can be done on a 32-bit micro-controller.

### 5.1 FUTURE WORK

Internet of Things will be a part of our daily lives. Energy constraineddevices and sensors will continuously be communicating witheach other the security of which must not be compromised. Security algorithm is proposed in our work named as IOT encryption. The implementation show promisingresults making the algorithm a suitable candidate to be adoptedin IoT applications. In the near future we are interested inthe detail performance evaluation and cryptanalysis of thisalgorithm on different hardware and software platforms for possible attacks.

## REFERENCES

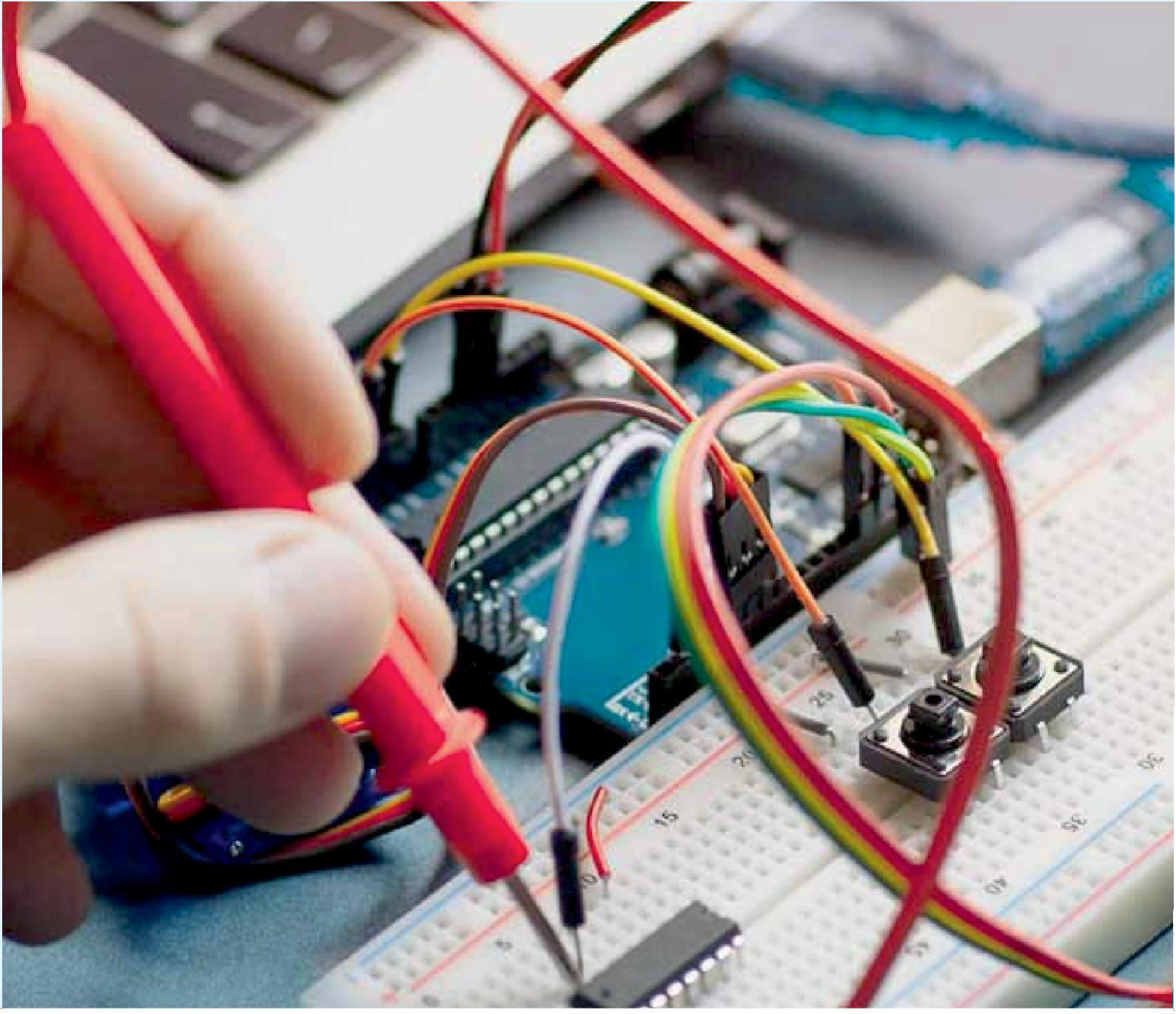
[1] KONG Liuyong, LI Lin "A new image encryption algorithm based on Chaos", Proceedings of the 35th Chinese Control Conference July 27-29, 2016,
[2] R. Want and S. Dustdar, "Activating the internet of things [guest editors' introduction]", Computer, vol. 48, no. 9, pp. 16–20, 2015.
[3] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major, and L. Kerr, "Security in the industrial internet of things", 2016.
[4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review", in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.
[5] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472.
[6] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.
[7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[8] L. Da Xu, "Enterprise systems: state-of-the-art and future trends," IEEETransactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.
[9] P. Barreto and V. Rijmen, "The khazad legacy-level block cipher," Primitive submitted to NESSIE, vol. 97, 2000.
[10] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things," Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.
[11] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystemanalysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.
[12] S. Misra, M. Maheswaran, and S. Hashmi, "Security challenges and approaches in internet of things," 2016.
[13] M. C. Domingo, "An overview of the internet of things for people with disabilities," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.
[14] W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologies of internet of things perceiving mine," Procedia Engineering, vol. 26, pp. 2326–2333, 2011.
[15] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," in Internet of Things. Springer, 2012, pp. 572–580.
[16] B. Karakostas, "A dns architecture for the internet of things: A case study in transport logistics," Procedia Computer Science, vol. 19, pp. 594–601, 2013.
[17] H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of security services for resource constrained internet of things," International Journal of Distributed Sensor Networks, vol. 2016, 2016.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|

||Volume 12, Issue 5, May 2023||

|DOI:10.15662/IJAREEIE.2022.1205024 |

[18] Jaiwei Han et.al 2001 Data Mining: concepts and Techniques, Morgan Kaugmann publishers
[19] P. L. L. P. Pan Wang, Professor SohailChaudhry, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337–359, 2016.
[20] M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer 2 peer system; an approach towards surmounting security challenges," arXiv preprint arXiv:1404.5123, 2014.



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.317

# International Journal of Advanced Research

## in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com



Scan to save the contact details