IMPLEMENTATION ON SECURITY IN IOT USING AN ENCRYPTION ALGORITHM

[1]Sadhna singh [2]Dr. Prashant Kumar Jain
[1]Student (M.E) [2]Professor & HOD
Department Of Electronics and Telecommunication Engineering
Jabalpur Engineering College, Jabalpur (M.P.),India

Abstract: The Internet of Things (IoT) being a promising technology of the future is expected to connect billions of devices. The increased rate of communication is able to generate mountains of data but the security of data can be a threat in itself. The devices in the architecture are essentially smaller in size and low powered. Conventional encryption algorithms are generally computationally expensive due to their complexity and requires many rounds to encrypt, essentially wasting the constrained energy of the gadgets. However, less complex algorithms may compromise the desired integrity. In this Paper we propose a light weight encryption algorithm named as Secure IoT (SIT).

Keyword: IoT, Key Encryption, Key Decryption, Key Expansion, Image Entropy, Key sensitivity.

1. INTRODUCTION

An important issue in digital transmission and storage is Security 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 is encryption get lower correlation in the pixel and gets the encrypted image. Many different image encryption techniques to protect confidential image data from unauthorized access is available. provide transmission of digital images in secure way. Algorithms that is good for textual data not 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 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 were used. Encryption which is useful 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

The many schemes used for enciphering 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. 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. Public key cryptography, keys work in pairs of matched public and private keys. Cryptography which can be used when secret messages are transferred from one party to 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 a one dimension 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, and 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 step. 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].

Addition operation for DNA sequence.

+	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

Subtraction operation for DNA sequence.

-	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C

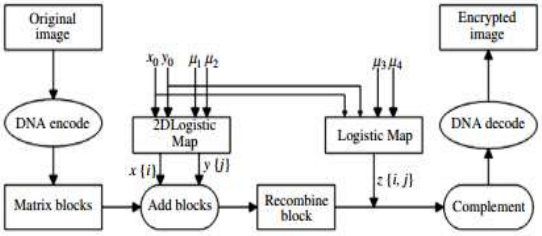

Fig.1 Block diagram for the image encryption algorithm.

2.PROBLEM FORMULATION

Method like DNA encryption the execution time for image encryption is higher and memory utilization increases on number of round discussed in previous work .in our proposed work we have tried to reduced execution and time memory utilization as well as 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 on 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.Algorithm is designed for IoT to deal with the security and resource utilization challenges mentioned

2.2.Objective

In proposed work we will minimize memory and run time along with less number of round for image encryption

3. 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 was done on Windows seven. 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 is actively operating behind the scenes.

4.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 a encryption algorithm named as IOT image encryption It is 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 is 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 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

4.3 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 Security key is assigned to input image encryption to make it more secure strong key selection is important for efficient encryption of imagePerformance 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

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.

1) Key Sensitivity:

An encryption algorithm must be sensitive to the key. It means that the algorithm must not retrieve the original data if the key has even a minute difference from the original key.Avalanche test is used to evaluate the amount of alterations occurred in the cipher text by changing one bit of the key or plain text. According to Strict Avalanche Criterion SAC if 50% of the bits are changed due to one bit change,the test is considered to be perfect. To visually observe this effect, we decrypt the image with a key that has a difference of only one bit from the correct key.

2) Execution Time:

One of the fundamental parameter for the evaluation of the algorithm is the amount of time it takes to encode and decode a particular data. The proposed algorithm is designed for the IoT environment must consume minimal time and offer considerable security.

3) Memory Utilization:

Memory utilization is a major concern in resource constrain IoT devices. An encryption algorithm 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.Smaller amount of memory engagement will be favourable for its deployment in IoT.

4) Image Entropy:

The encryption algorithm adds extra information to the data so as to make it difficult for the intruder to differentiate between the original information and the one added by the algorithm. We measure the amount of information in terms of entropy, therefore it can be said that higher the entropy better is the performance of security algorithm.

5) Correlation:

The correlation between two values is a statistical relationship that depicts the dependency of one value on another. Data points that hold substantial dependency has a significant correlation value. A good cipher is expected to remove the dependency of the cipher text from the original message. Therefore no information can be extracted from the cipher alone and no relationship can be drawn between the plain text and cipher text. This criterion is best explained by Shannon in his communication theory of secrecy systems.

4.4 Simulation And Results.

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 require to lower the correlation between adjacent pixels.

4.5 Algorithm

Step1.Key Expansion for five rounds
Step2.After the generation of round keys the encryption process can be started.
Step 3.check execution time.
Step 4. Check Memory Utilization.
Step 5 Measures the amount of information in terms of entropy,
Step 6 Calculate the correlation coefficient for original and encrypted images.
Step 7 comparisons of results.

FLOW CHART OF METHODOLOGY

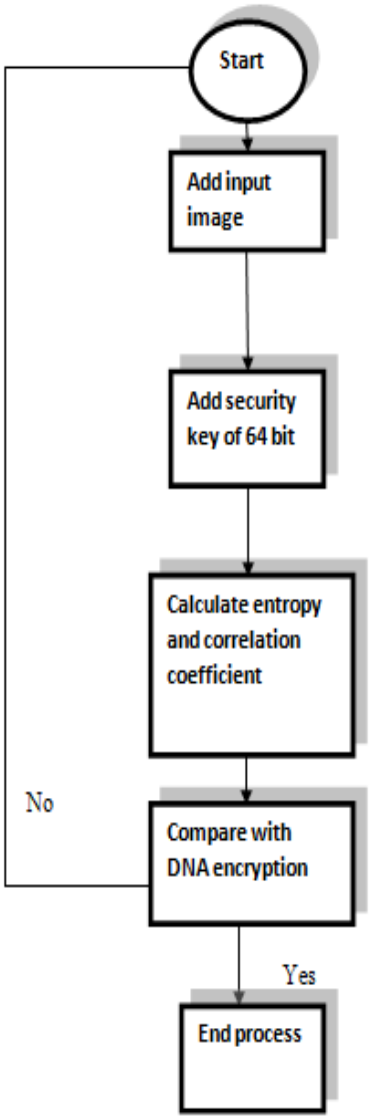

Fig 1 MATLAB RESULTS

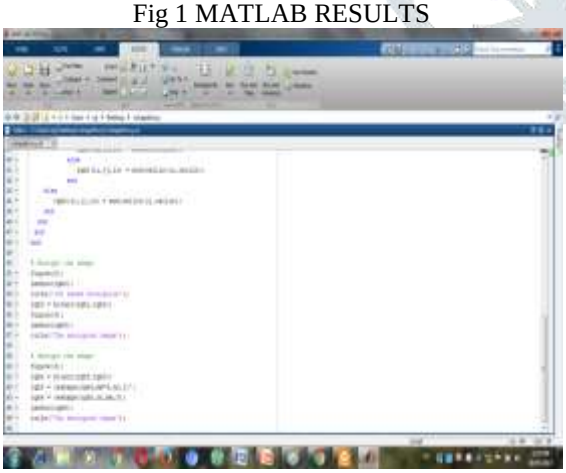

Fig 2 Used Programing In Matlab

Fig 3 Image sample

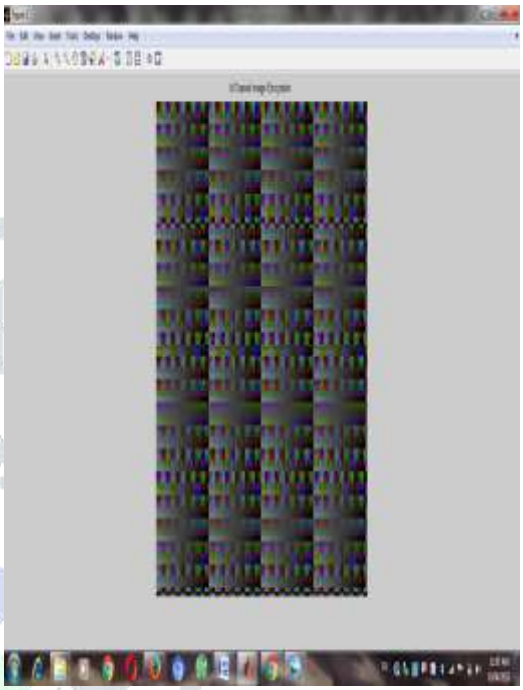

Fig 4 Corelation of Image

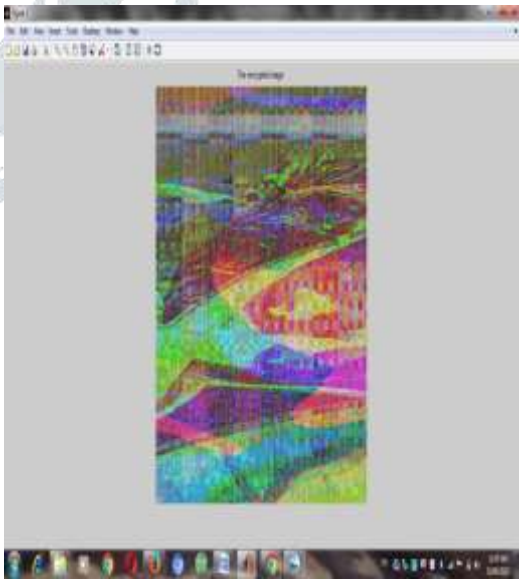

Fig 5 Corelation & Entropy of Image

Fig 6 Final Result of Image

4.6 Result Comparison

An encryption algorithm discussed in base paper 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 on ATmega 328 platform While for DNA encryption the software environment is MATLAB2014a, the hardware environment is the win7 system, the processor is i5, the RAM is 4GB, and the hard disk is PC with 500G. With the above simulation environment, simulation and analysis are carried out for the secret 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 IOT Performance
Entropy	7.9979	7.9977	Satisfactory(almost equal)
Correlation	0.015 (High)	0.0015 (low)	Excellent than DNA
Memory cost	RAM4G(Cost High)	ATmega328 Low cost	Excellent than DNA

Proposed work based on IOT has five rounds of calculation which makes proposed method better than DNA based image Encryption The execution time is found to be 0.188 milliseconds and 0.187 milliseconds for encryption and decryption respectively which is less than DNA based methodology which has more rounds consumes more time

DNA encryption gets the entropy of information: 7.9979 which is closed to IoT based entropy around 7.9977 but memory cost and run time consume more than IoT

5. CONCLUSION

The communication is expected to generate data and the security of data can be a threat. The devices in the architecture are smaller in size and low powered. Old encryption algorithms are generally computationally expensive due to their complexity and requires many rounds to encrypt, essentially wasting the constrained energy of the gadgets. Less complex algorithm,Simulations result shows the algorithm provides substantial security in just five encryption rounds. The hardware implementation of the algorithm is done on a 32-bit micro-controller

FUTURE WORK

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

REFERENCES

[1] KONG Liuyong, LI Lin "A new image encryption algorithm based on ChaosProceedings 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," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.

[9] P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam, and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.

[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.
[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.
[21] M. A. SimplicioJr, M. V. Silva, R. C. Alves, and T. K. Shibata,
"Lightweight and escrow-less authenticated key agreement for the internet of things," *Computer Communications*, 2016.
[22] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
[23] F. Xie and H. Chen, "An efficient and robust data integrity verification
algorithm based on context sensitive," *way*, vol. 10, no. 4, 2016.
[24] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," *International Journal of Sustainable Development & World Ecology*, vol. 20, no. 3, pp. 216–222, 2013.
[25] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (rfid) systems," *NIST Special publication*, vol. 80, pp. 1–154, 2007
[26] Lynch C., "Big data: how do your data grow?" Nature. 455, (7209), 28 –29 (2008).CrossRef

[27]Refregier P., and Javidi B., "Optical image encryption based on input plane and Fourier planerandom encoding," Opt. Lett.. 20, (7), 767 –769 (1995). 0146-9592 CrossRef

[28]Stu G., and Zhang J., "Multiple-image encryption by wavelength multiplexing," Opt. Lett.. 30, (11), 1306 –1308 (2005). 0146-9592 CrossRef

[29]Poon T.-C., and Banerjee P. P., Contemporary Optical Image Processing with MATLAB. , Elsevier , Oxford (2001).

[30]Wang Q. et al., "Double image encryption using phase-shifting interferometry and random mixed encoding method in fractional Fourier transform domain," Opt. Eng.. 52, (8), 084101 (2013).CrossRef

[31]Chang H. T. et al., "Wavelength multiplexing multiple-image encryption using cascaded phase-only masks in the Fresnel transform domain," Appl. Opt.. 50, (5), 710 –716 (2011). 0003-6935 CrossRef

[32]Tao R., , Xin Y., and Wang Y., "Double image encryption based on random phase encoding in the fractional Fourier domain," Opt. Express. 15, (24), 16067 –16079 (2007). 1094-4087 CrossRef

[33]Di H. et al., "Multiple-image encryption by compressive holography," Appl. Opt.. 51, (7), 1000 –1009 (2012). 0003-6935 CrossRef

[34]Kim D.-H. et al., "Crosstalk analysis for multiple-image encryption and image-quality equalization technology," Microsyst. Technol.. 21, (12), 2717 –2725 (2015). 0946-7076 CrossRef

[35]Liu Z. et al., "Optical multi-image encryption based on frequency shift," Opt. Int. J. Light Electron Opt.. 122, (11), 1010 –1013 (2011).CrossRef

[36]Sui L. et al., "Asymmetric double-image encryption method by using iterative phase retrieval algorithm in fractional Fourier transform domain," Opt. Eng.. 53, (2), 026108 (2014).CrossRef

[37]Rawat N. et al., "Compressive sensing based robust multispectral double-image encryption," Appl. Opt.. 54, (7), 1782 –1793 (2015). 0003-6935 CrossRef

[38]Walther A., "The question of phase retrieval in optics," Opt. Acta Int. J. Opt.. 10, (1), 41 –49 (1963).CrossRef

[39]Fienup J. R., "Phase retrieval algorithms: a comparison," Appl. Opt.. 21, (15), 2758 –2769 (1982). 0003-6935 CrossRef

[40]Fienup J. R., "Reconstruction of an object from the modulus of its Fourier transform," Opt. Lett.. 3, (1), 27 –29 (1978). 0146-9592 CrossRef

[41]Wu L., , Tao S., and Xiao S., "Phase retrieval-based distribution detecting method for transparent objects," Opt. Eng.. 54, (11), 113103 (2015).CrossRef

[42]Teague M. R., "Deterministic phase retrieval: a Green's function solution," J. Opt. Soc. Am.. 73, (11), 1434 –1441 (1983). 0030-3941 CrossRef

[43]Gerchberg R. W., and Saxton W. O., "A practical algorithm for the determination of the phase from image and diffraction plane pictures," Optik (Stuttg). 35, , 237 (1972). 0030-4026