Application of a lightweight Encryption Algorithm to a quantized speech image for Secure IoT

Mourad Talbi[1], Med Salim Bouhalel[2]

[1]Center of Researches and Technologies of Energy of Borj Cedria, Tunis, Tunis

[2]Sciences Electroniques, Technologie de l'Information et Télécommunications (SETIT)

[1]mourad.talbi@crten.rnrt.tn, [2]mbouhlel@gmail.com

Abstract—The IoT Internet of Things being a promising technology of the future. It is expected to connect billions of devices. The increased communication number is expected to generate data mountain and the data security can be a threat. The devices in the architecture are fundamentally smaller in size and low powered. In general, classical encryption algorithms are computationally expensive and this due to their complexity and needs numerous rounds for encrypting, basically wasting the constrained energy of the gadgets. Less complex algorithm, though, may compromise the desired integrity. In this paper we apply a lightweight encryption algorithm named as Secure IoT (SIT) to a quantized speech image for Secure IoT. It is a 64-bit block cipher and requires 64-bit key to encrypt the data. This quantized speech image is constructed by first quantizing a speech signal and then splitting the quantized signal into frames. Then each of these frames is transposed for obtaining the different columns of this quantized speech image. Simulations result shows the algorithm provides substantial security in just five encryption rounds.

Keywords—IoT, Security, Encryption, quantized speech image, SNR, PESQ, Histogram, Entropy, Correlation.

1. Introduction

In the latest years, the Internet of Things (IoT) is turning out to be an emerging discussion in the research domains and practical implementation. IoT is a model including ordinary entities with the ability to sense and communicate with corresponding devices using Internet [1]. Nowadays, the broadband Internet is generally accessible to any user and its cost of connectivity is also reduced, more sensors and gadgets are getting connected to it [2]. Such conditions are providing suitable ground for the IoT growth. There are many research works focussing on complexities around the IoT and we wish to approach any object from anywhere in the world [3]. The sophisticated sensors and chips are embedded in the physical things surrounding us, each transmitting valuable data. The sharing process of such large amount of data begins with the devices themselves which should securely communicate with the IoT platform. The latter integrates the data from many devices and applies analytic computations to share the most valuable data with the applications. The IoT is taking the mobile network, conventional internet and sensor network to another level as everything will be connected to the internet. A matter of concern that should be kept under consideration is to guarantee the issues related to data integrity, confidentiality and authenticity that will emerge on security account and privacy [4, 5].

1.1. Applications of IoT:

With revolution of telecommunication, more and more devices are getting connected to the Internet. A great number of devices such as the personal computer, tablets laptops, smart phones, smart TVs, video game consoles even the refrigerators and air conditioners have the ability to communicate with each other or over Internet. This trend is extending outwards and it was estimated that by the year 2020 there will be over 50 billion objects connected to the Internet [6]. This estimates that for each person in the world there will be 6.6 objects online [1]. The world will be blanketed with millions of sensors gathering information from physical objects and will upload it to the Internet. It is suggested that IoT application is yet in the early phase but is beginning to evolve fast [7, 8]. In [9], is given an IoT overview in building automation system. In [10], it is suggested that a variety of industries have a growing interest towards IoT use. Different IoT applications in healthcare industries are presented in [11, 12] and the development opportunities in healthcare brought in by IoT will be huge [13].

It is predicted that IoT will contribute in the making the mining production safer [14] and the forecasting of disaster will be made possible. It was expected that IoT will transform the automobile services and transportation systems [15].

Since more physical objects will be equipped with sensors and RFID tags, transportation companies will be capable to track and monitor the object movement from origin to destination [16]. Therefore, IoT shows promising performance in the logistics industry as well. With a great number of applications eyeing to adapt the technology with the intentions to contribute in the economy growth, healthcare facility, transportation and a better life style for the public, IoT should provide adequate security to their data for encouraging the adaptation process [1].

1.2. Security Challenges in IoT

To adopt the IoT technology it is essential to build the confidence among the users about its security and privacy that it will not cause any serious threat to their data integrity, authority and confidentiality. Intrinsically IoT is vulnerable to a variety of sorts of security threats, if needed, security measures are not taken there will be a threat of information leakage or could prove a damage to economy [17, 18]. Such threats can be considered as one of the main hindrance in IoT [19, 20]. IoT is very open to attacks [21, 22], for the arguments that there is a fair possibility of physical attack on its components as they remain unsupervised for long time. Secondly, due to the wireless communication medium, the eavesdropping is very simple [1].

Finally the constituents of IoT bear low competency in terms of computational capability and as well as in terms of energy with which they are operated. The implementation of conventional computationally expensive security algorithms will lead to the hindrance on the performance of the energy constrained devices [1].

It is predicted that substantial amount of data is expected to be generated while IoT is used for monitoring purposes and it is vital to preserve unification of data [23]. Precisely, data integrity and authentication are the matters of concern. From a high level perspective, IoT is composed of three components namely, Hardware, Middleware and Presentation [1]. Hardware consists of sensors and actuators, the Middleware provides storage and computing tools and the presentation provides the interpretation tools accessible on different platforms. It is not feasible to process the data collected from billions of sensors, context-aware Middleware solutions are proposed to help a sensor decide the most important data for processing [24]. Inherently the architecture of IoT does not offer sufficient margin to accomplish the necessary actions involved in the process of authentication and data integrity. The devices in the IoT such as RFID are questionable to achieve the fundamental requirements of authentication process that includes constant communication with the servers and exchange messages with nodes. In secure systems the confidentiality of the data is maintained and it is made sure that during the process of message exchange the data retains its originality and no alteration is unseen by the system. The IoT is composed of many small devices such as RFIDs which remain unattended for extended times, it is easier for the adversary to access the data stored in the memory [25]. To provide the immunity against Sybil attacks in RFID tags, received signal strength indication (RSSI) based methodologies are used in [26], [27], [28] and [29]. Many solutions have been proposed for the wireless sensor networks which consider the sensor as a part of Internet connected via nodes [30]. However, in IoT the sensor nodes themselves are considered as the Internet nodes making the authentication process even more significant. The integrity of the data also becomes vital and requires special attention towards retaining its reliability [1].

1.3. Motivation And Organization of Paper

Recently a study by HP reveals that 70% of the devices in IoT are vulnerable to attacks [31]. An attack can be performed by sensing the communication between two nodes which is known as a man-in-the-middle attack. No reliable solution has been proposed to cater such attacks. Encryption however 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. Various cryptographic algorithms have been developed that addresses the said matter, but 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. A trade-off must be done to fulfil the requirement of security with low computational cost [1].

2. Cryptographic Algorithms For IoT

The need for the lightweight cryptography have been extensively discussed [32, 33], as well the shortcomings of the IoT in terms of constrained devices are highlighted. In fact there are some lightweight cryptography algorithms that doesn’t always use security-efficiency trade-offs. Amongst the block cipher, stream cipher and hash functions, the block ciphers have proved significantly their better performances. A novel block cipher called mCrypton, is proposed in [34]. The cipher comes with the options of 64 bits, 96 bits and 128 bits key size. The architecture of this algorithm is followed by Crypton [35]. Though, functions of each component are simplified to enhance its performance for the constrained hardware. In [36], the successor of Hummingbird-1 [37] was proposed as Hummingbird-2(HB-2). With 128 bits of key and a 64 bit initialization vector Hummingbird-2 is tested to stay unaffected by all of the previously known attacks. Although, the cryptanalysis of HB-2 [38] highlights the weaknesses of the algorithm and that the initial key can be recovered. In [39] were studied different legacy encryption algorithms including RC4, IDEA and RC5 and their energy consumption was measured. They calculated the computational cost of the RC4 [40], IDEA [41] and RC5 ciphers on diverse platforms. Though, a variety of existing algorithms were omitted during this study.

- TEA [42], Skipjack [43] and RC5 algorithms have been implemented on Mica2 hardware platform [44]. For determining the energy consumption and memory use of the ciphers Mica2 was configured in single mote. Some block ciphers including AES [45], XXTEA [46], Skipjack and RC5 have been implemented [47], the energy consumption and execution time is determined. The results show that in the AES algorithm, the key size has great impact on the encryption phases, decryption and key setup i-e the longer key size results in extended execution process. RC5 provides diversified parameters i-e key size, rounds number and word size can be altered. Authors have performed various combinations to realize that it took longer time to execute when the word size is increasing.

As the key setup phase is not involved in XXTEA and Skipjack, they drew less energy but their security strength is not as much as RC5 and AES. In [48] was proposed lightweight block cipher Simon and Speck to show optimal results in software and hardware respectively. Both ciphers offer a range of key size and width, but at least 22 numbers of round need to perform enough encryption. Though, the Simon is based on low multiplication complexity. However, the total number of required mathematical operation is quite high [49, 50].

3. The proposed Algorithm

In this paper we propose to apply a lightweight Encryption Algorithm to a quantized speech image for Secure Internet of Things. This application is justified by the following arguments:

- We need to send confidential data between many devices with high level security,
- A lightweight Encryption Algorithm can be implemented in simple devices which don't require powerful processors,

The construction of a quantized speech image is illustrated in Figure 1. According to this figure, the different steps of this construction are given as follow:

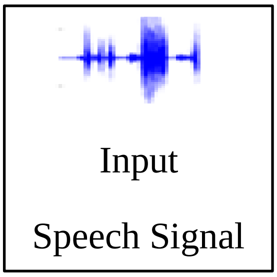
1. Quantization of the input speech signal,
2. Splitting the obtained quantized speech signal into frames where each of them is of length N. These frames are in number of N and are noted as follow: $F_i, 1 \leq i \leq N$,
3. Transpose each of these frames $F_i, 1 \leq i \leq N$ in order to obtain the different columns $V_i, 1 \leq i \leq N$ of this quantized speech image, $\mathrm{V} = [\mathrm{V}_1 \mathrm{V}_2 \dots \mathrm{V}_{\mathrm{N}-1} \mathrm{V}_{\mathrm{N}}]$,

In figure 2 is illustrated the block diagram of the proposed encryption/decryption technique applied to the quantized speech image for Secure Internet of Things.
As shown in Figure 2, a lightweight encryption algorithm proposed in [5], is applied to the quantized speech image in order to obtain the encrypted image. After that, the lightweight decryption algorithm [5] is applied to the encrypted image in order to have the decrypted image. Then, the reconstruction of the quantized speech signal is performed and finally the de-quantization is applied to this signal in order to obtain the output speech signal which represents the confidential data.

4. Experimental Setup

To test the security strength of the proposed technique, it is evaluated on the basis of the following criterion:

- effect of cipher on the entropy
- Key sensitivity
- Histogram and correlation of the image.



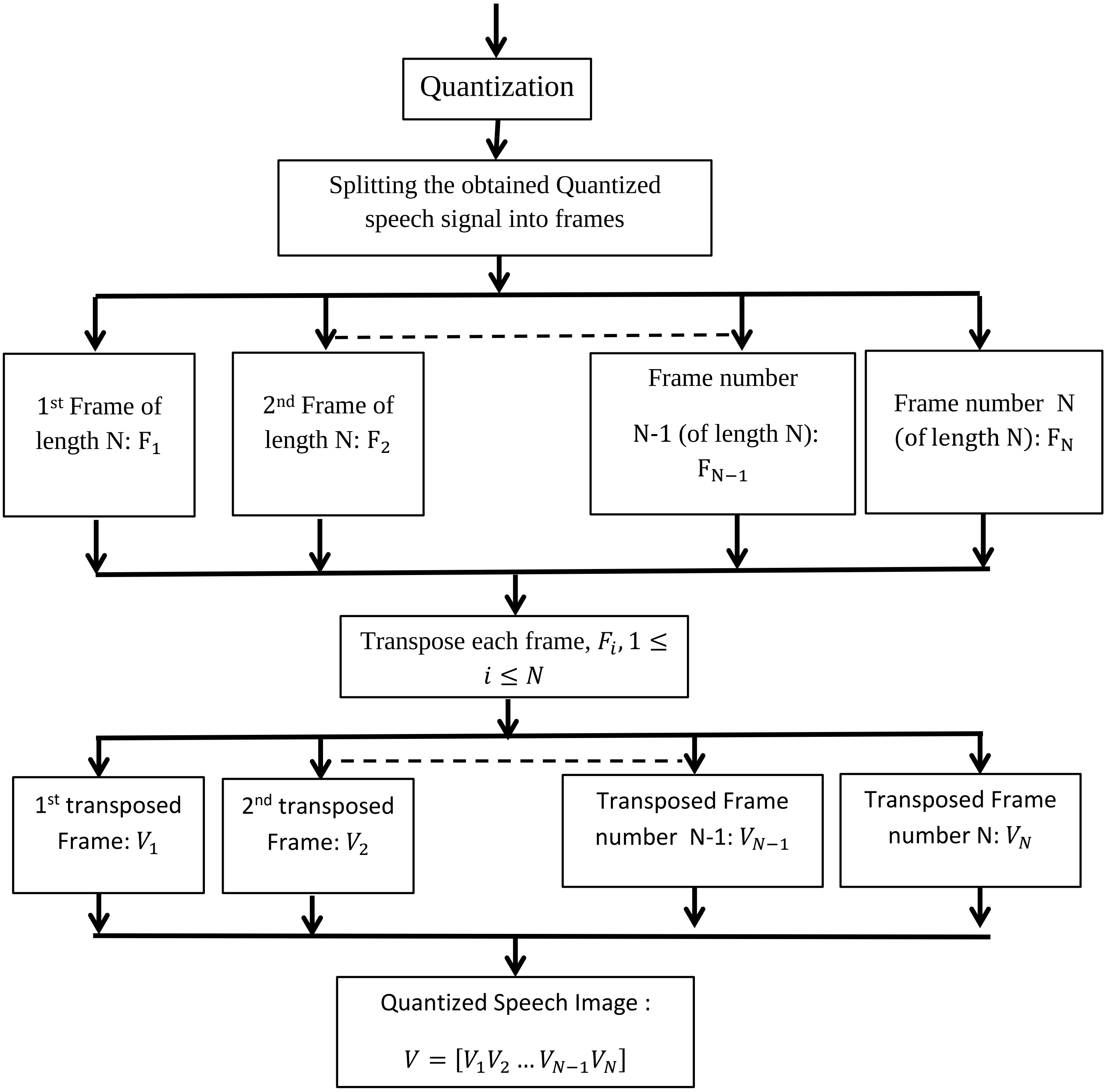
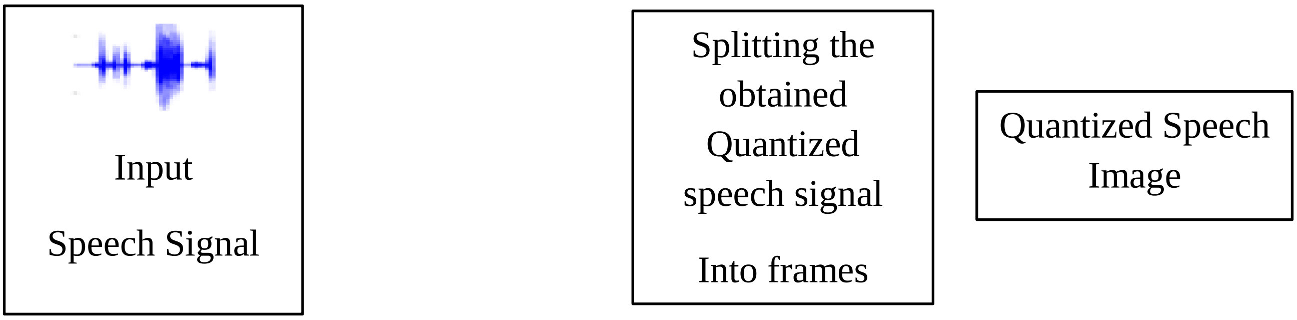

Quantization
Splitting the obtained Quantized speech signal into frames
1st Frame of length N: F_1
2nd Frame of length N: F_2
Frame number N-1 (of length N): F_{N-1}
Frame number N (of length N): F_N
Transpose each frame, $F_i, 1 \leq i \leq N$
1st transposed Frame: V_1
2nd transposed Frame: V_2
Transposed Frame number N-1: V_{N-1}
Transposed Frame number N: V_N
Quantized Speech Image :
$V = [V_1V_2 \dots V_{N-1}V_N]$

Figure 1. The block diagram of the construction of a quantized speech image.



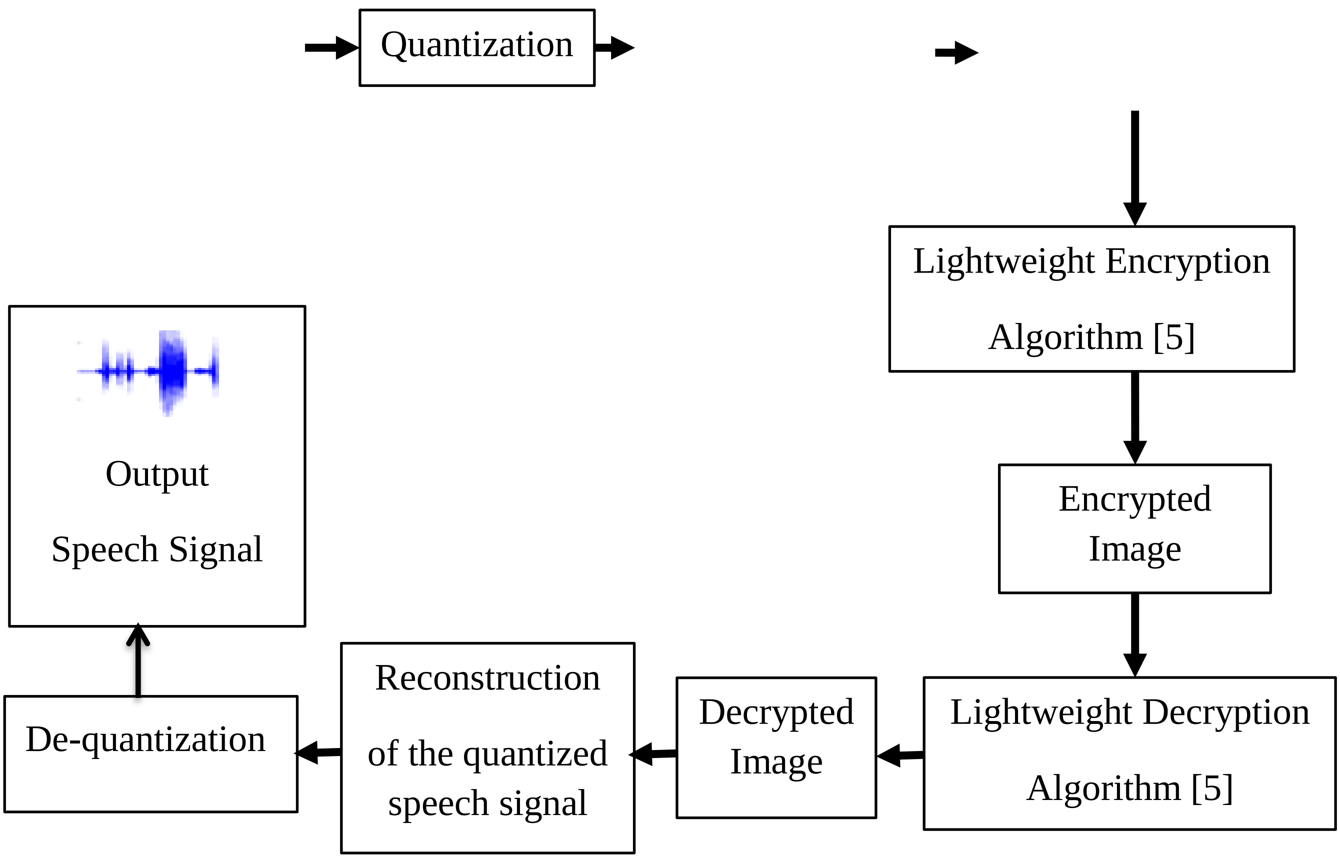

Quantization
Lightweight Encryption Algorithm [5]
Encrypted Image
Lightweight Decryption Algorithm [5]
Decrypted Image
Reconstruction of the quantized speech signal
De-quantization
Output Speech Signal

Figure 2. the block diagram of the proposed encryption technique applied to the quantized speech image for Secure Internet of Things.

We further tested this technique 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.

- Key Sensitivity: An algorithm of encryption should be sensitive to the key. It means that it should not retrieve the original data when the key has even a minute difference from the original key. Avalanche test is employed 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 [66] when 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.

- Execution Time: One of the fundamental parameter for the algorithm evaluation is the time amount that it takes for encoding and decoding a particular data. The algorithm proposed in [5] is designed for the IoT environment sould consume minimal time and provide substantial security [5].

- Memory Utilization: Memory utilization is a principal concern in resource constrain IoT devices. An encryption algorithm is composed of some computational rounds that may occupy significant memory making it inappropriate to be used in IoT. Consequently, the proposed technique is evaluated in terms of its memory utilization. Smaller memory amount engagement will be favourable for its deployment in IoT.

- Image Histogram: A method for observing visual effect of the cipher is to encrypt an image with the proposed algorithm and view the randomness it produces in the image. For evaluating the generated randomness, the image histogram is computed. after encryption, a uniform histogram depicts appreciable security.

- Image Entropy: The encryption algorithm adds extra information to the data so that mak it difficult for the intruder to differentiate between the original information and the one added by the algorithm. The information amount is measured in terms of entropy, consequently it can be said that higher the entropy better is the security algorithm performance. For measuring the entropy (H) for an image, equation (1) is applied on the intensity (I) values and $P(I_i)$ is the intensity value probability I_i.

$$H(I) = -\sum_{i=1}^{2^8} P(I_i) log_b\big(P(I_i)\big) \qquad (1)$$

- Correlation: The correlation between two values represents 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 eliminate the dependency of the cipher text from the original message [5]. Consequently, no information can be extracted from the cipher alone and no relationship can be drawn between cipher text and the plain text [5]. Shannon has explained this criterion in his communication theory of secrecy systems [67].

In this experiment we calculated the correlation coefficient for original and encrypted images. The correlation coefficient for original and encrypted images. The correlation coefficient $'\Upsilon$ is computed by employing equation (2). For ideal cipher case $'\Upsilon$ have to be equal to 0 and the worst case $'\Upsilon$ will be equal to 1.

$$'\Upsilon_{x,y} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \qquad (2)$$

With $D(y)$, $D(x)$ and $cov(x,y)$, are respectively the variances and covariance of the variables y and x. The spread of values or variance of any single dimension random variable can be computed by employing the equation (3).

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)^2 \qquad (3)$$

With $D(x)$ represents the variance variable x.

The covariance between two random variables x and y, $cov(x,y)$ s expressed as follow:

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \qquad (4)$$

In equations 3 and 4, the quantities $E(y)$ and $E(x)$ represents respectively the expected values of the random variables y and x. These expectations are computed by using the following formula:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (5)$$

With N is the total number of pixels in the image and is equal to $row \times col$, x is a vector having N as length and x_i represents the ith intensity values of the original image.

For testing the perceptual quality of the reconstructed speech signal, we use in this work the Signal to Noise Ratio (SNR) and the PESQ (Perceptual evaluation of Speech Quality) where their definitions were given in many references such as is [53].

5. Results and Discussion

According to [5] the algorithm simulation is made in order to perform the standard tests including Avalanche and image entropy and histogram on Intel Core i7-3770@3.40 GHz processor employing MATLAB®. For evaluating the performance in the real IoT environment, Muhammad Usman et al. Implemented the algorithm on ATmega 328 based Arduino Uno board as well. The memory utilization and execution time of their proposed algorithm [5] was observed. In [5], the execution time was found to be respectively 0.188 millisconds for encryption and 0.187 milliseconds for decryption, the algorithm proposed in [5] employs the 22 bytes of memory on ATmega 328 platform. As previously mentioned, in this work, we use the same encryption/decryption algorithms proposed in [5]. The encryption algorithm proposed in [5] was compared with other algorithms implemented on hardware as shown in table 1 [5].

Table 1. Results for Hardware implementations [5].

CIPHER	DEVICE	Block Size	Key Size	Code Size	RAM	Cycles (ene)	Cycles (dec)
AES [68]	AVR	64	128	1570	-	2739	3579
HIGHT [69]	AVR	64	128	5672	-	2964	2964
IDEA [70]	AVR	64	80	596	-	2700	15393
KATAN [70]	AVR	64	80	338	18	72063	88525
KLEIN [70]	AVR	64	80	1268	18	6095	7658
PRESENT [71]	AVR	64	128	1000	18	11342	13599
TEA [70]	AVR	64	128	648	24	7408	7539
PRINCE [71]	AVR	64	128	1574	24	3253	3293
SKIPJACK [72]	Power TOSSIM	64	80	5230	328	17390	-
RC5 [72]	Power TOSSIM	64	128	3288	72	70700	-
SIT	ATmega328	64	64	826	22	3006	2984

Key and Block sizes are in bits whereas RAM and code size are in bytes. The cycles include key expansions along with both encryption and decryption [5].

The Avalanche test of the algorithm shows that a single bit change in key or plain text brings around 49% change in the cipher bits, which is close to the ideal 50% change. The results in [5] show that the precise decryption is possible merely when the correct key is employed for decrypting the encrypted image. When the incorrect key is employed, the image remains non recognizable. For a visual demonstration of Avalanche test, compared to the original key, the wrong key has a difference of just a bit, the algorithm strength can be perceived from this result.

To perform histogram and entropy tests, in this work we have used a speech signal ''original1.wav'' represented in Figure 4. From results in Table 2, it can be remarked that the entropy of the encrypted image is greater than the original image. The correlation comparison in Figure 9 illustrates the contrast between the encrypted and the original data. The original data which is in our work the quantized speech image. This image is highly correlated and detaining a high value for the correlation coefficient. However, the encrypted image does not seem to have any correlation.

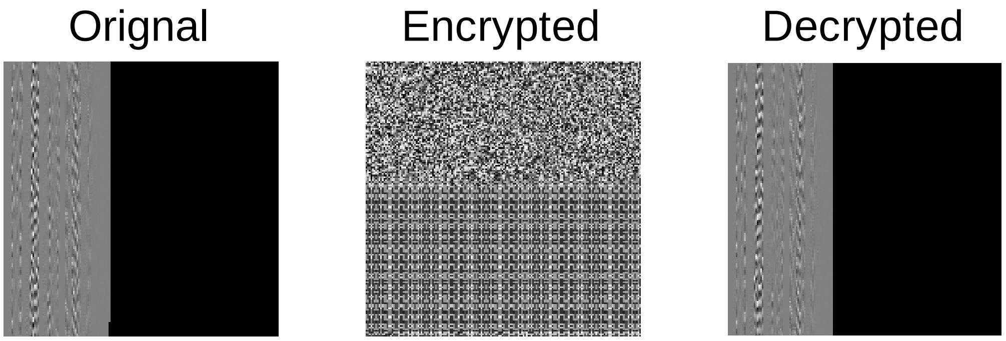


Figure 3. Image Encrypted/Decrypted

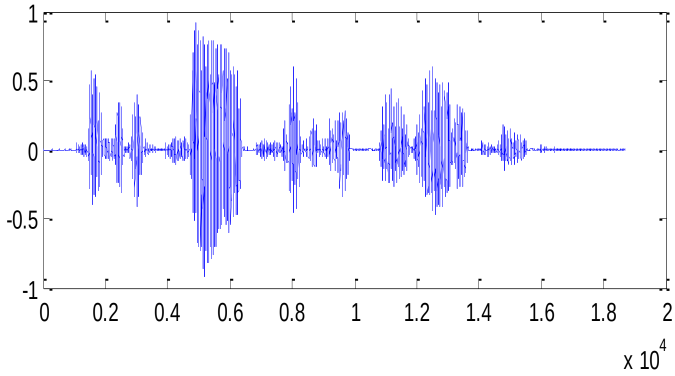


Figure 4. Original Speech Signal.

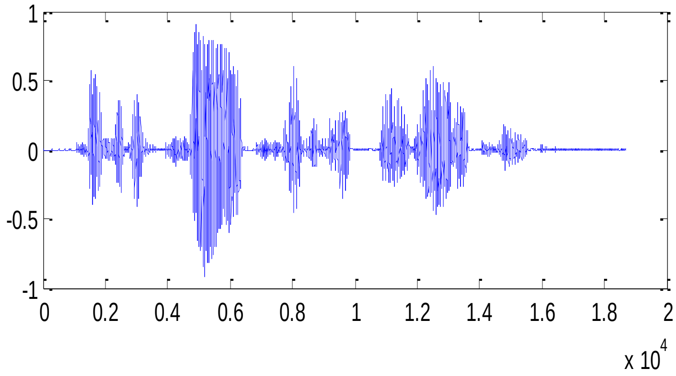
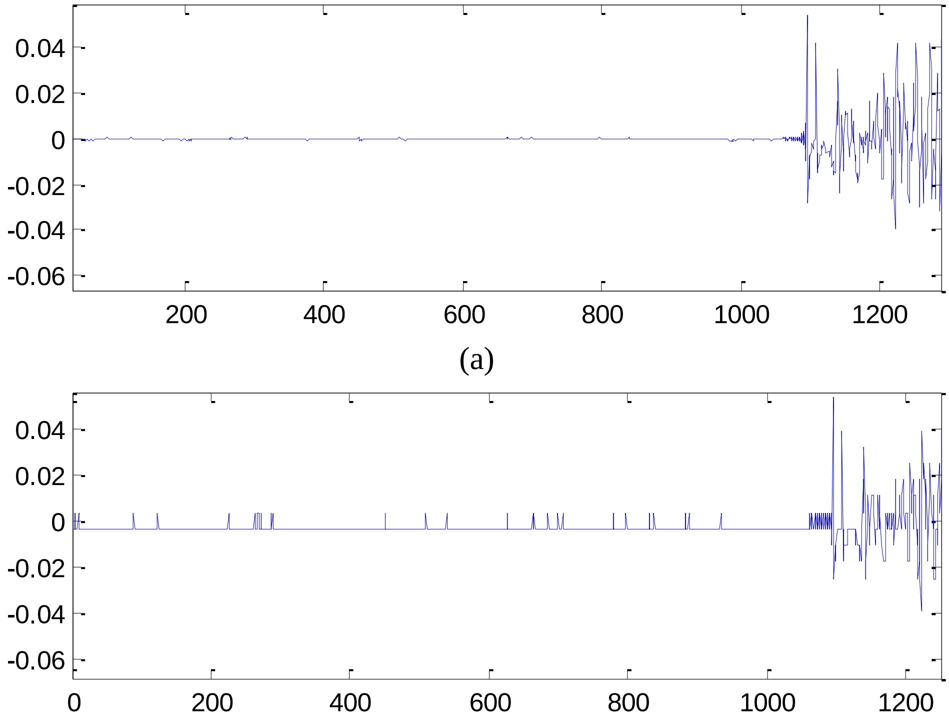


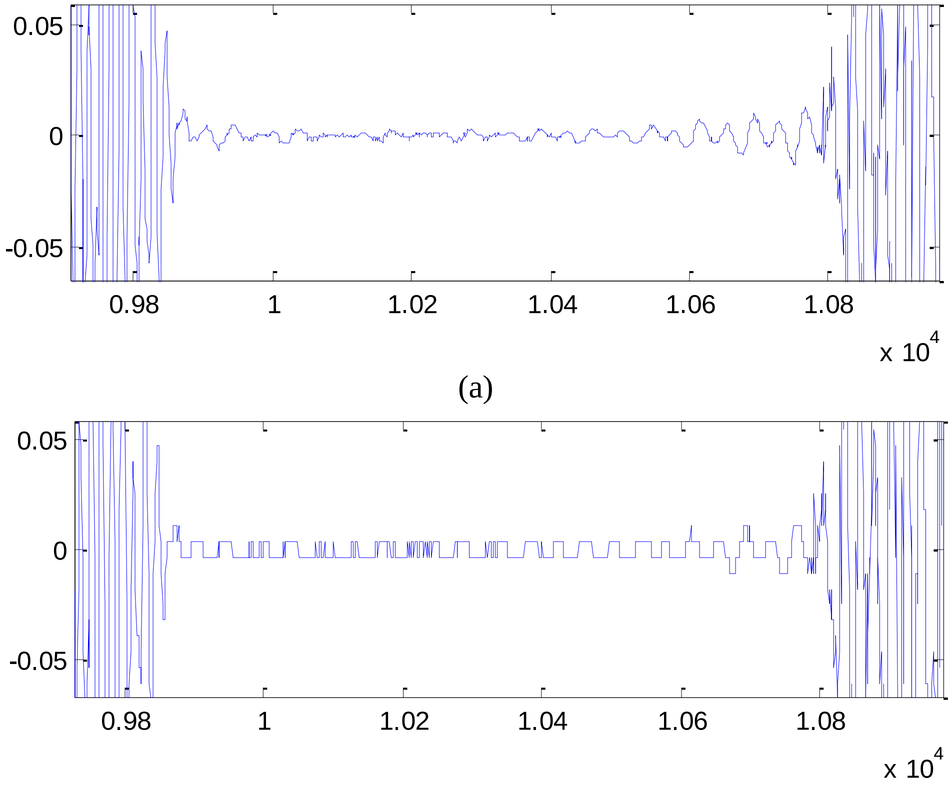
Figure 5. Reconstructed Speech Signal after Decrypted and Dequantization.



(a)

(b)

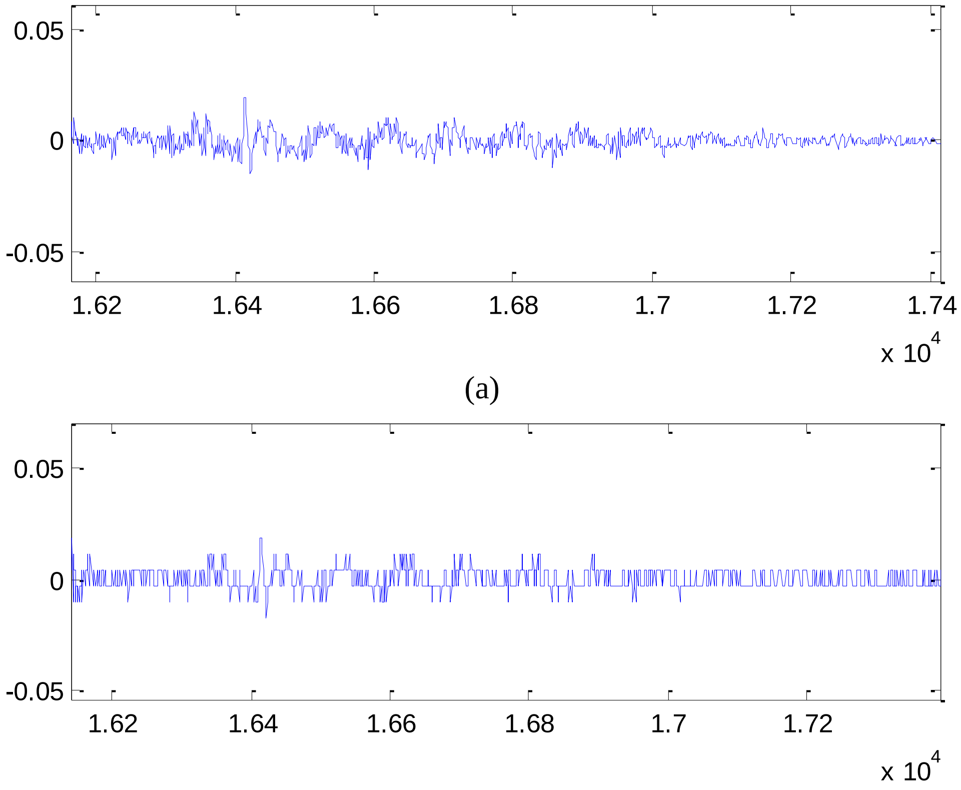
Figure 6. (a) The beguining of the original speech signal (Zoomed), (b) the same region of the reconstructed speech signal after Decrypted and Dequantization (Zoomed).



(a)

(b)

Figure 7. The middle of the original speech signal (Zoomed), (b) the same region of the reconstructed speech signal after Decrypted and Dequantization (Zoomed).

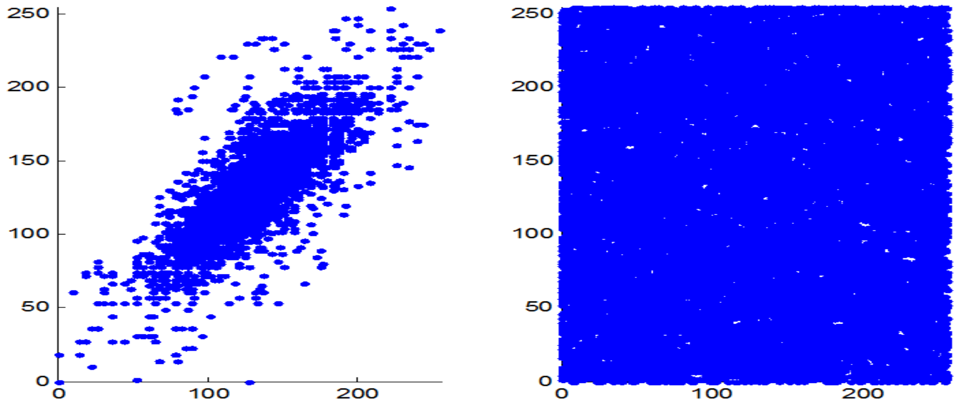


(a)

(b)

Figure 8. The end of the original speech signal (Zoomed), (b) the same region of the reconstructed speech signal after Decrypted and Dequantization (Zoomed).

Figures 6 to 8 show clearly the difference between the original speech signal and the reconstructed speech one obtained after decryption and dequantization. This difference is due to quantization/dequantization.



Original quantized speech image

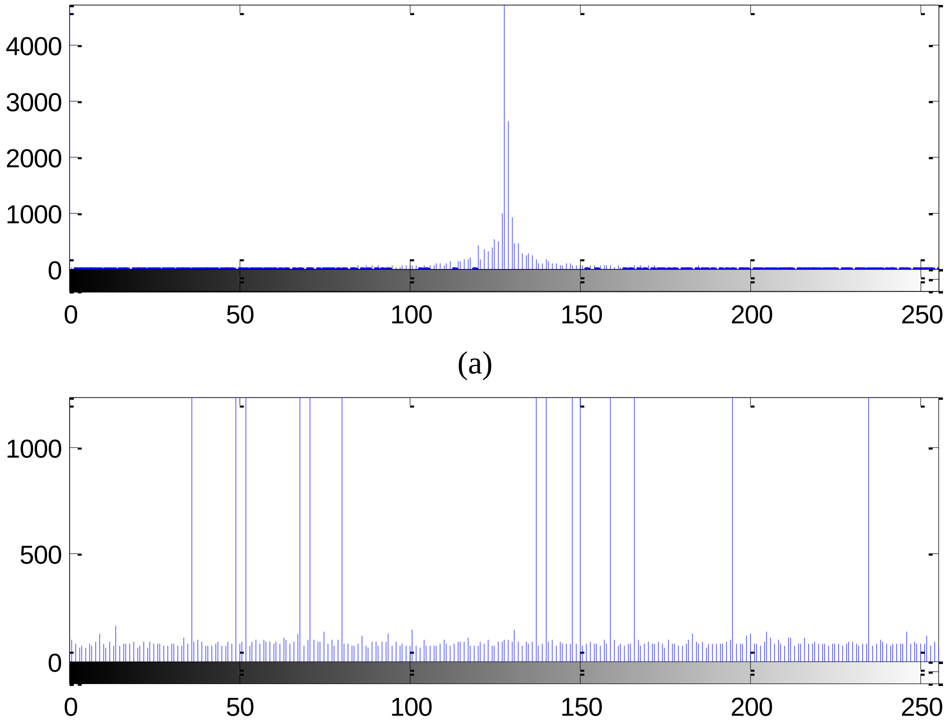
Encrypted quantized speech

Figure 9. Correlation comparison.

Table 2. Results for Correlation and Entropy.

Speech Signal	Size of the Quantized Speech Image	Correlation		Entropy		SNR (dB)	PESQ
		Original Quantized Speech Image	Encrypted Quantized Speech Image	Original Quantized Speech Image	Encrypted Quantized Speech Image	SNR of the Reconstructed Speech signal	PESQ of the Reconst -ructed Speech signal
'original 1.wav'	220×220	0.9952	0.0255	2.7560	6.4783	33.9532	3.9794
Total encryption time (in Second)							
27.753251							

According to the results obtained from SNR and PESQ computations (Table 2), the reconstructed speech signal is with very good perceptual quality.



(a)

(b)

Figure 10. (a) Histogram of the original Speech quantized Image, (b) Histogram of the Encrypted Speech quantized Image

In the results of histogram in Figure 10 for the original and encrypted image, the almost uniform distribution of intensities after the encryption is an indication of desired security.

6. **Conclusion**

In the near future Internet of Things will be an important element of our daily lives. Many energy constrained devices and sensors will continuously be communicating with each other and the security of which must not be compromised. For this reasonn a lightweight security algorithm is to a quantized speech image for Secure IoT. This quantized speech image is constructed by first quantizing a speech signal and then splitting the quantized signal into frames. Then each of these frames is transposed for obtaining the different columns of this quantized speech image. The simulations show promising results making the algorithm a suitable candidate to be adopted in IoT applications.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[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] Muhammad Usman, Irfan Ahmedy, M. Imran Aslamy, Shujaat Khan and Usman Ali Shahy, ‘‘SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,’’ International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.
[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, “Ecosystem analysis 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] S. Khan, M. Ebrahim, and K. A. Khan, “Performance evaluation of secure force symmetric key algorithm,” 2015.
[19] P. L. L. P. Pan Wang, Professor Sohail Chaudhry, 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. Simplicio Jr, 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] J. Wang, G. Yang, Y. Sun, and S. Chen, “Sybil attack detection based on rssi for wireless sensor network,” in 2007 International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2684–2687.
[27] S. Lv, X. Wang, X. Zhao, and X. Zhou, “Detecting the sybil attack cooperatively in wireless sensor networks,” in Computational Intelligence and Security, 2008. CIS’08. International Conference on, vol. 1. IEEE, 2008, pp. 442–446.
[28] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and localizing identity-based attacks in wireless and sensor networks,” IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418–2434, 2010.
[29] S. Chen, G. Yang, and S. Chen, “A security routing mechanism against sybil attack for wireless sensor networks,” in Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 142–146.
[30] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 41–47.
[31] S. A. Kumar, T. Vealey, and H. Srivastava, “Security in internet of things: Challenges, solutions and future directions,” in 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781.
[32] M. Katagi and S. Moriai, “Lightweight cryptography for the internet of things,” Sony Corporation, pp. 7–10, 2008.
[33] M. Ebrahim, S. Khan, and S. S. U. H. Mohani, “Peer-to-peer network simulators: an analytical review,” arXiv preprint arXiv:1405.0400, 2014.
[34] C. H. Lim and T. Korkishko, “mcrypton–a lightweight block cipher for security of low-cost rfid tags and sensors,” in Information Security Applications. Springer, 2005, pp. 243–258.
[35] C. H. Lim, “Crypton: A new 128-bit block cipher,” NIsT AEs Proposal, 1998.
[36] D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith, “The hummingbird-2 lightweight authenticated encryption algorithm,” in RFID. Security and Privacy. Springer, 2011, pp. 19–31.
[37] D. Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith, “Ultralightweight cryptography for low-cost rfid tags: Hummingbird algorithm and protocol,” Centre for Applied Cryptographic Research (CACR) Technical Reports, vol. 29, 2009.

[38] K. Zhang, L. Ding, and J. Guan, "Cryptanalysis of hummingbird-2." IACR Cryptology ePrint Archive, vol. 2012, p. 207, 2012.
[39] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications. ACM, 2003, pp. 151–159.
[40] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.
[41] X. Lai, "On the design and security of block ciphers," Ph.D. dissertation, Diss. Techn. Wiss ETH Z¨urich, Nr. 9752, 1992. Ref.: JL Massey; Korref.: H. B¨uhlmann, 1992.
[42] D. J. Wheeler and R. M. Needham, "Tea, a tiny encryption algorithm," in Fast Software Encryption. Springer, 1994, pp. 363–366.
[43] E. Brickell, D. Denning, S. Kent, D. Maher, and W. Tuchman, "The skipjack algorithm," Jul, vol. 28, pp. 1–7, 1993.
[44] E. Souto, D. Sadok, J. Kelner et al., "Evaluation of security mechanisms in wireless sensor networks," in null. IEEE, 2005, pp. 428–433.
[45] A. E. Standard, "Federal information processing standards publication 197," FIPS PUB, pp. 46–3, 2001.
[46] D. J. Wheeler and R. M. Needham, "Correction to xtea," Unpublished manuscript, Computer Laboratory, Cambridge University, England, 1998.
[47] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," Computer Networks, vol. 54, no. 17, pp. 2967–2978, 2010.
[48] B. Ray, S. Douglas, S. Jason, T. Stefan, W. Bryan, and W. Louis, "The simon and speck families of lightweight block ciphers," Cryptology ePrint Archive, Report./404, Tech. Rep., 2013.
[49] T. Mourouzis, G. Song, N. Courtois, and M. Christofii, "Advanced differential cryptanalysis of reduced-round simon64/128 using largeround statistical distinguishers," 2015.
[50] S. Khan, M. S. Ibrahim, K. A. Khan, and M. Ebrahim, "Security analysis of secure force algorithm for wireless sensor networks," arXiv preprint arXiv:1509.00981, 2015.
[51] A. Webster and S. E. Tavares, "On the design of s-boxes," in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1985, pp. 523–534.
[52] C. E. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.
[53] Mourad Talbi, ''Speech enhancement based on stationary bionic wavelet transform and maximum a posterior estimator of magnitude-squared spectrum,'' International Journal of Speech Technology, March 2017, Volume 20, Issue 1, pp 75–88.