A Lightweight PSIS Scheme Based on Multi-node Collaboration in the IoT

Lina Zhang[1,2], Bo Yang[1(✉)], Tao Wang[1], and Tong Wang[2]

[1] Shaanxi Normal University, Xi'an 710119, Shaanxi, China
zhangln@xust.edu.cn, {byang,water}@snnu.edu.cn
[2] Xi'an University of Science and Technology, Xi'an, Shaanxi, China

Abstract. Traditional threshold-based SIS schemes can no longer meet some application scenarios. In contrast, Progressive Secret Image Sharing (PSIS) schemes have been continuously studied. In order to meet the different data storage methods in the nodes in the IoT, as well as the small size and limited energy of the nodes, a lightweight PSIS scheme based on multi-node collaboration in the IoT is proposed. This solution gradually recovers the secret image through the collaboration of multiple nodes in the IoT, which overcomes the drawbacks of the traditional threshold schemes and also brings convenience to the secure transmission of secret images in the IoT. Experiments have proved that the scheme has certain practicability.

Keywords: IoT · PSIS · Multi-node · Modulo operations · Interpolated polynomial

1 Introduction

IoT is a network based on information carriers such as the Internet and traditional telecommunications networks, allowing all ordinary physical objects that can be independently addressed to achieve interconnection [1]. As information carrier, images are widely used in various fields. Especially in the related applications of IoT, image security issues are particularly important.

The perception nodes are important part of IoT [2–4]. It is mainly responsible for information collection, data fusion and data transmission. As a result, it has attracted much attention of the criminals and are extremely vulnerable to physical capture and brute force cracking. Once a node in the IoT is cracked, the attacker has the legal identity to use the network and launches an internal attack, pouring massive amounts of redundant data into the network, causing network congestion. From this point of view, malicious nodes within the network pose agreat threat. Therefore, it is extremely urgent to focus on a secure transmission algorithm of IoT node information with low complexity and high compatibility [5]. Low complexity mainly includes three aspects: (1) the verification method is simple, the verifier can complete the verification of nodes data only through

W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 77–87, 2022.
https://doi.org/10.1007/978-3-030-96791-8_6

the exclusive OR operation. (2) the space complexity is low, the local data of nodes will be uploaded to the cloud before being used, and the verifier uses corresponding shares to check, so the space complexity is 0(1). Compatibility is reflected in the nodes that store different data. Before the result is reconstructed, the nodes are independent of each other, but when the result is reconstructed, the nodes cooperate to provide effective data and complete the result aggregation. To sum up, a lightweight PSIS scheme based on multi-node collaboration in the IoT is proposed, which is designed to protect image content, reduce energy consumption of nodes, and perform lightweight authentication between nodes.

Shamir was the first to propose (k, n) threshold secret sharing [6]. With the continuous development of research, the research trend of SIS schemes is divided into two branches: the traditional (k, n) threshold SIS schemes [7–9] and PSIS schemes [10–12]. The traditional schemes provides an all-or-nothing recovery mode, and PSIS can gradually recover the secret image. Actually, The former needs to meet two characteristics: (1) no image information can be obtained with less than k shadows, (2) the entire secret can be gained with any k shadows. For PSIS schemes, in addition to satisfying the above two characteristics, another feature must be satisfied: after obtaining any k shadows, each additional shadow will restore a new part of the image content.

The perception nodes in the IoT are deployed in any possible position. In addition, these nodes have limited energy and volume, thus, they are prone to damage and malicious attacks. Once the node holding the secret share is destroyed or its energy is completely lost, the traditional (k, n) SIS scheme will not be able to recover the original image. On the contrary, for PSIS scheme, the loss of part of the secret shares will not affect the restoration of the original image content.

Recently, researchers have proposed various PSIS schemes [10,12–16]. The work in [10] proposes a new scalable (t, s, k, n) SIS scheme with essential shadows, where k or more shadows which include at least t essential shadows can gradually reconstruct secret image. Entire secret image can be reconstructed when all s essential shadows are involved. This scheme combines the features of SIS and PSIS. The approach in [12] develops a new (k, n) PSIS based on polynomial with smaller shadow size. This method has good smoothness during recovery, however, it is not fine-grained enough. The study in [13] proposes a general (k, n) Scalable SIS (SSIS) scheme with the smooth scalability. However, its smoothness is still not good enough.

In this paper, we propose a lightweight PSIS scheme based on multi-node collaboration in the IoT. The main contributions of this paper are as follows:

1) Combined with modulo operation, a multi-interlaced spiral matrix is designed.
2) A fine-grained PSIS scheme is proposed.
3) The scheme is designed based on the multi-node collaboration in the IoT. It can transmit image data securely while also performing mutual authentication between nodes.

4) Performance with fault tolerance. The reason is that the (k, n) threshold design scheme is used in the scheme, which allows the falsified data submitted by $n-k$ nodes out of n nodes to be tolerant of $\frac{n-k}{k}$.

The rest of this paper is organized as follows: In next section, we prepare some preliminaries, which include basic theory of secret sharing, Thien-Lin SIS scheme [17], scalable SIS (SSIS) scheme [13], and the design of multi-interleaved spiral matrix based on modular arithmetic. In Sect. 3, we propose a lightweight PSIS scheme based on multi-node collaboration in the IoT. In Sect. 4, experimental results and analyses are used to show the performance and superiority of the proposed scheme. Comparisons with related works are given in Sect. 5. The conclusion is included in Sect. 5.

2 Preliminaries

In this section, basic theory of secret sharing, two representive SIS schemes that are Thien-Lin SIS scheme [15] and PSIS scheme [26], and the design of multi-interleaved spiral matrix based on modular arithmetic are introduced.

2.1 Basic Theory of Secret Sharing

The basic theory of secret sharing was first proposed by Shamir [14]. Let *GF(q)* be a finite field, where q is a large prime number that satisfies $q \geq n+1$. The secret S is a random number uniformly selected on $GF(q)\backslash\{0\}\,(i = 1, 2, 3, \cdots, k)$, denoted as $S \leftarrow {}_R GF(q)\backslash\{0\}\,(i = 1, 2, 3, \cdots, k)$. Construct a $k-1$-degree polynomial on $GF(q)$ as $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$.

The n participants are denoted as $P_1, P_2, P_3, \cdots, P_n$. Their assigned secret share is $f(i)(i = 1, 2, 3, \cdots, n)$. For any k participants $P_{i_1}, P_{i_2}, \cdots, P_{i_k}, i_j \in [1, n], j = 1, 2, \cdots, k$, when they want to obtain the secret s, they can utilize $f(i_j)$ to construct a linear equation system as Eq. (1).

$$\begin{aligned} a_0 + a_1 i_1 + \cdots + a_{k-1} i_1^{k-1} &= f(i_1) \\ a_0 + a_1 i_2 + \cdots + a_{k-1} i_2^{k-1} &= f(i_2) \\ &\vdots \\ a_0 + a_1 i_k + \cdots + a_{k-1} i_k^{k-1} &= f(i_k) \end{aligned} \tag{1}$$

Since the value of i_j is different, Eq. (2) can be constructed according to the Lagrange interpolation formula:

$$f(x) = \sum_{j=1}^{k} f(i_j) \prod_{\substack{l=1 \\ l \neq j}}^{k} \frac{(x - i_l)}{(i_j - i_l)} \pmod{q} \tag{2}$$

Therefore, the secret $S = f(0)$ can be obtained from Eq. (3).

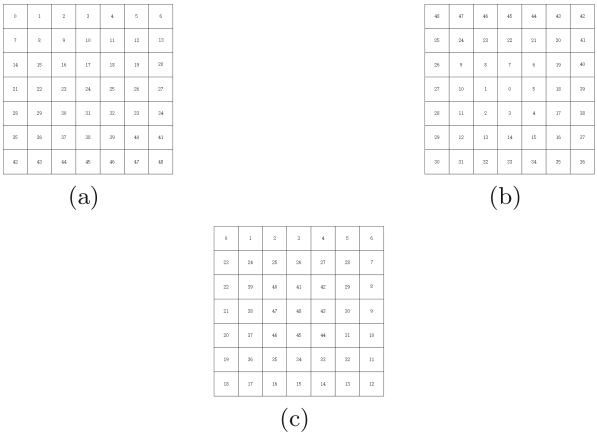
$$S = (-1)^{k-1} \sum_{j=1}^{k} f(i_j) \prod_{\substack{l=1 \\ l \neq j}}^{k} \frac{i_l}{i_j - i_l} \pmod{q} \tag{3}$$

2.2 Thien-Lin SIS Scheme

Thien and Lin propose an SIS scheme in [15]. By dividing the image pixels into non-overlapping sections and each section has k pixels. Then, the Lagrangian interpolation polynomial is constructed. The pixels of each section are used as the coefficients of the Lagrangian interpolation polynomial to generate multiple shares.

2.3 The Spiral Matrix

In order to recover the secret image in a fine-grained manner during the recovery phase, we combine modular arithmetic to design a multi-interlaced spiral matrix, see Fig. 1(c). The matrix can perform fine-grained block division of the image to be processed. The most obvious advantage is that the image blocks restored each time look uniform and random. Figure 1 shows three special matrices, where the numbering of (a) is sequential, and the numbering of (b) and (c) is spiral. Bessides, they are divided into clockwise and counterclockwise spiral matrices according to the direction of rotation. According to the starting position of the number, they are divided into spiral matrices from outside to inside and from inside to outside. Except for the different order of numbers, the basic rules of these spiral matrices are similar.



(a) (b) (c)

Fig. 1. Three types of matrices

In this paper, we will use the method shown in Fig. 1(c) to segment and number the image. Then, the restoration of secret image can achieve a more fine-grained progressive method. Besides, the recovered content looks very random. In fact, the matrix shown in Fig. 1(a) can also achieve fine-grained recovery, however, its recovery results do not seem to be random enough.

3 The Proposed Scheme

With the rapid development of the Internet, IoT and cloud computing have also emerged. Therefore, information security has become particularly important. How to ensure the security of image information in the IoT is one of the problems to be solved in this paper. As shown in Fig. 2, cloud computing layer: high-speed computing equipment with large-scale, distributed, high-availability, scalability and security; Edge computing layer: computing terminal equipment with light weight, high performance, low power consumption, flexible configuration of computing power, convenient access, etc.; IoT device layer: basic devices with computing and perception characteristics. The data collected at the IoT device layer need to be calculated and processed. Then, they will be uploaded to the cloud server. The safe transmission and storage of data during the whole process is very important.

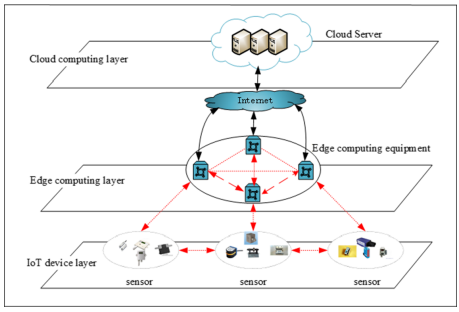


Fig. 2. The spiral matrix

Therefore, a lightweight PSIS scheme based on multi-node collaboration in the IoT is proposed in this paper. This scheme divides the secret image into multiple shares and stores them in different nodes. Our proposed scheme can not only perform mutual authentication between nodes, but also ensure the safe transmission and storage of images.

The proposed scheme is divided into two phases: the sharing phase and recovery phase, the implementation details are as follows.

Sharing Phase

1. Divide the secret image(note: IoT device completed).
   Divide the secret image I with size $a \times b$ into m non-overlapping blocks equally. Then, use the method shown in Fig. 1 to number these blocks, marked as

$I_1, I_2, I_3, \cdots, I_m$. Besides, all of these blocks should meet two conditions as Eq. (5)

$$\begin{cases} I = \bigcup_i I_i & ,i = 1, 2, 3, \cdots, m. \\ I_i \bigcap I_j = \varnothing & ,1 \leq i \neq j \leq m. \end{cases} \tag{4}$$

2. Generate the sub-images(note: Edge layer device implementation).
Perform modular operation on the numbers corresponding to these m sub-images. According to the related knowledge of number theory, $a \pmod b = c$, where $0 \leq c < b$ and a, b, c are all positive integers. Therefore, we perform modular operations on m numbers respectively in this paper. Then, $q \pmod M$ and $q \pmod N$ two operations shoule be performed, where $q = 1, 2, 3, \cdots, m$ and $M = k, N = k^2$. Specifically as shown in Eq. 6.

$$\begin{cases} I_1^{'} = \bigcup_t I_t, t \in [1, m], t(modM) = 0 \\ I_2^{'} = \bigcup_t I_t, t \in [1, m], t(modN) = 1 \\ \vdots \\ I_j^{'} = \bigcup_t I_t, t \in [1, m], t(modN) = q \\ q \neq k \times i, q \leq N - 1, n \in [1, n] \end{cases} \tag{5}$$

In Eq. (6), $I_1^{'}, I_2^{'}, \cdots, I_j^{'}$ are the sub-images. Note that the value q should satisfy $q \neq pi$ and $i = 1, 2, 3, \cdots$. In addition, the size of these sub-images should satisfy Eq. (7).

$$size(I_j^{'}) = \begin{cases} \frac{1}{k}|I|, j = 1 \\ \frac{1}{k^2}|I|, j \in [2, N-1] \end{cases} \tag{6}$$

3. Generate n sub-shadows for each sub-image(note: Cloud computing layer equipment completed).
For $I_1^{'}$, we use Thien-Lin (k, n) SIS to generate n sub-shadows $s_{1,1}, s_{1,2}, s_{1,3}, \cdots, s_{1,n}$.
For $I_j^{'}, (j \geq 2)$, we use Thien-Lin $(k + j - 1, n)$ SIS to generate n sub-shadows $s_{j,1}, s_{j,2}, s_{j,3}, \cdots, s_{j,n}$.
4. Generate n shadow images. Besides, our standard parameter for setting the module is 257 in Thien-Lin $(k + j - 1, n)$ SIS.
The final n shadow images $S_i = s_{1,i} \cup s_{2,i} \cup s_{3,i} \cup \cdots \cup s_{n,i}, i = 1, 2, 3, \cdots, n$.

Note that the shadow size is $|S_i| = \frac{|I|}{n}(1 + \sum_{l=k+1}^{n} \frac{1}{l}), i = 1, 2, 3, \cdots, n$. Finally, we store n shadow images in different nodes and perform authentication between nodes if necessary, or upload them to the cloud server for analysis and processing.

Recovery Phase

In the recovery phase, there need at least k shadow images to recover the secret image. As the share increases, more content can be recovered. Until all shadow images participate in the restoration, the secret image can be completely restored. The difference in the number of shares leads to different recovery results. There are $n - k + 1$ cases of recovery results. Suppose there are currently s shadow images involved in the reconstruction. The specific process is as follows.

1. $s = k$. A $k - 1$-degree polynomial is constructed. Next, a linear equation system like Eq. (1) is constructed. Then, the sub-image $I_1^{'}$ can be obtained by solving the k coefficients of the equation system. Finaly, we put the blocks that make up $I_1^{'}$ back to the original positions to recover part of the original image. Note that only sub-image $I_1^{'}$ can be recovered from these k shadow images.
2. $s = k + j - 1, j \geq 2$. Similarly, we should construct several polynomials:

$$
\begin{aligned}
&f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}. \\
&f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_k x^k. \\
&\vdots \\
&f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k+j-2} x^{k+j-2}.
\end{aligned}
$$

Then, we construct the corresponding linear equations according to these polynomials. The sub-image $I_1^{'}, I_2^{'}, \cdots, I_j^{'}$ can be obtained by solving the coefficients of the equation system respectively. Similarly, the corresponding image content can be restored by placing these blocks of these sub-images in their original positions.

Theorem 1. *Each shadow image gives no clue about the secret image.*

Proof. We construct several Langerange interpolation polynomials in the sharing phase, namely the shadow image generation process, and the pixels of the secret image are taken as the coefficients of the polynomials.

Theorem 2. *Any set of less than k shadow images cannot obtain any information about the secret image.*

Proof. In short, any set of less than k shadow images cannot obtain any information about the secret image.

Theorem 3. *Any set of t* $(k \leq t < n)$ *shadow images can decode the secret image in a degree.*

Proof. In short, any set of t $(k \leq t < n)$ shadow images can decode the secret image in a degree.

Theorem 4. *Only when all the shadow images are involved in the reconstruction can the secret image be completely recovered*

Proof. According to **Theorem** 3, each sub-image along with the entire secret image can be recovered if all shadow images are involved in the reconstruction.

4 Experimental Results and Example

4.1 Experimental Results

In the section, we take "Lena" as an example to analyze the performance of the proposed method, the size of "Lena" is 372 × 372, which is shown in Fig. 3. This example is done with $k = 3$, $n = 9$. First, we should divide "Lena" into no overlapping blocks of equal size, which is shown in Fig. 4. Here, the block size is 12×12, we mark the blocks in Fig. 4 in a spiral manner, denoted as M. When $(M \bmod 3) = 0$, sub-image Q_1 is generated. Then, when $(M \bmod 9) = 1$, $(M \bmod 9) = 2$, $(M \bmod 9) = 4$, $(M \bmod 9) = 5$, $(M \bmod 9) = 7$ and $(M \bmod 9) = 8$, sub-image Q_2, Q_3, Q_4, Q_5, Q_6, Q_7 are generate shown in Fig. 5. Next, encrypt each subgraph Q_j, j ∈ [1, 7].

Fig. 3. Secret S_1

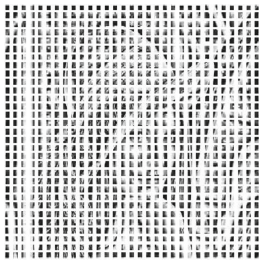


Fig. 4. Segment image

(a) Q_1

(b) Q_2

(c) Q_3

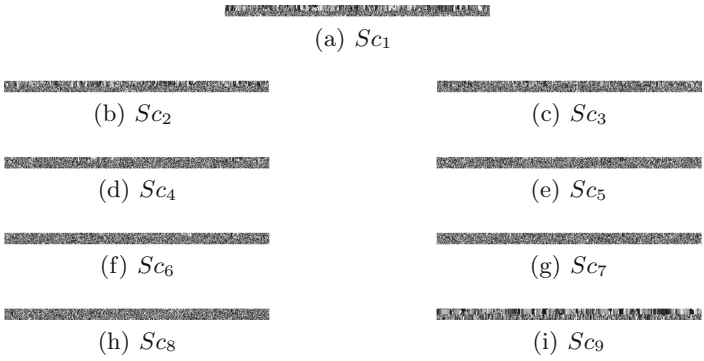
(d) Q_4

(e) Q_5

(f) Q_6

(g) Q_7

Fig. 5. Seven sub-images



(a) Sc_1 (b) Sc_2 (c) Sc_3 (d) Sc_4 (e) Sc_5 (f) Sc_6 (g) Sc_7 (h) Sc_8 (i) Sc_9

Fig. 6. Nine shadow images

In the encryption phase, we encrypt the subgraph Q_j according to different thresholds. The encryption threshold of each sub-image is expressed as Q_j^{k+j-1}, j $\in [1, 7]$ (note: the subgraph Q_j is encrypted with $(k+j-1, n)$ threshold). Assign the shadows Sc_1, Sc_2, Sc_3, Sc_4, Sc_5, Sc_6, Sc_7, Sc_8, Sc_9 to 9 participants. The result is shown in Fig. 6.

The process and effects of the recovery phase are consistent with the schemes described.

4.2 Example

We use scalable ($k = 3$, $n = 9$) threshold to encode secret image S_2. Through our scheme processing, the secret image c generates 7 subgraphs Q_j, j $\in [1, 7]$.

Assume that Q_1 consists of three 3 pixels blocks $B_{1,1} = (210, 211, 213)$, $B_{1,2} = (215, 215, 216)$, $B_{1,3} = (231, 217, 185)$. Q_2 is one 4-pixels block, $B_{2,1} = (233, 207, 211, 212)$. Q_3 is one 5-pixels block, $B_{3,1} = (215, 211, 196, 193, 199,)$. Q_4 is one 6-pixels block, $B_{4,1} = (249, 168, 128, 84, 89, 105)$. Q_5 consists of one 7-pixels block, $B_{5,1} = (102, 105, 108, 222, 223, 224, 226)$. Q_6 is one 8-pixels block, $B_{6,1} = (176, 179, 180, 181, 183, 186, 190, 195)$. Q_7 consists of one 9-pixels block, $B_{7,1} = (159, 162, 164, 167, 168, 166, 166, 165, 165)$.

Encoding Phase

for sub-image Q_1 generate three 2 degree polynomials:

$$\begin{aligned} f_{1,1}(x) &= (210 + 211x^1 + 213x^2) mod 257 \\ f_{1,2}(x) &= (215 + 215x^1 + 216x^2) mod 257 \\ f_{1,3}(x) &= (231 + 217x^1 + 185x^2) mod 257 \end{aligned} \tag{7}$$

for each block $B_{1,1}$, $B_{1,2}$, $B_{1,3}$ respectively, and then compute the values $f_{1,i}(j)$, $i \in [1, 3]$, $j \in [1, 9]$. Thus the sub-shadow $s_{1,j}$, $j \in [1, 9]$, for each participant P_j is $s_{1,j} = (f_{1,1}(j), f_{1,2}(j), f_{1,3}(j))$.

For sub-images Q_2, Q_3,..., Q_7 generate $f_{2,1}(x) = (223 + 207x^1 + 211x^2 + 212x^3) mod 257$, $f_{3,1}(x) = (215+211x^1+196x^2+193x^3+199x^4) mod 257$, $f_{7,1}(x) = (159+162x^1+164x^2+167x^3+168x^4+166x^5+166x^6+165x^7+165x^8) mod 257$, respectively. The subshadow $s_{2,j}$, $s_{3,j}$, ..., $s_{7,j}$, $j \in [1, 9]$. For each participant P_j is $s_{2,j} = f_2(j)$, $s_{3,j} = f_3(j)$,..., $s_{7,j} = f_7(j)$.

The nine shadows $SC_j, j \in [1, 9]$ are:

$$\begin{aligned} SC_1 &= (s_{1,1}, s_{2,1}, s_{3,1}, s_{4,1}, s_{5,1}, s_{6,1}, s_{7,1}) \\ &= ([120, 132, 119], 82, 243, 52, 182, 185, 189) \\ SC_2 &= (s_{1,2}, s_{2,2}, s_{3,2}, s_{4,2}, s_{5,2}, s_{6,2}, s_{7,2}) \\ &= ([199, 224, 120], 93, 238, 128, 221, 129, 35) \\ &\cdots \\ SC_9 &= (s_{1,9}, s_{2,9}, s_{3,9}, s_{4,9}, s_{5,9}, s_{6,9}, s_{7,9}) \\ &= ([87, 114, 207], 250, 197, 165, 230, 235, 251) \end{aligned} \tag{8}$$

Decoding Phase

The secret image S_2 can be reconstructed from 3 to 9 shadows under progress model. Any 3 shadows can reconstruct sub-image Q_1, any 4 shadows can reconstruct the 4-pixels block, then sub-image Q_2 can be extracted together with Q_1, any 5 shadows can reconstruct Q_1, Q_2 and Q_3, any 6 shadows can reconstruct Q_1, Q_2, Q_3, Q_4. As the number of shadows increases, all subimages Q_1, Q_2, Q_3, Q_4, Q_5, Q_6, Q_7 are restored losslessly. So, all seven shadows can reconstruct the entire secret image $S_2 = Q_1||Q_2||Q_3||Q_4||Q_5||Q_6||Q_7$.

5 Conclusion

With the rapid development of the Internet, people's lives are increasingly dependent on it. For example, IoT based on the Internet has been widely applied to many aspects of life, such as transportation, security, medical care, manufacturing, agriculture, and so on. However, in the related applications of the IoT, security issues have become a focus of attention. A lightweight PSIS scheme based on multi-node collaboration in the IoT is proposed. Generally speaking, the proposed scheme can recover the entire secret image in a fine-grained manner. The difference from the existing schemes is that it is global progressive. Actually, the recovery process can also be used as a batch authentication of nodes. In addition, the size of the secret share generated by the secret image is smaller than that of the original image. Therefore, the energy of the nodes can be saved during storage or transmission. In summary, our proposed method is suitable for related applications of the IoT.

References

1. Ammar, M., Russello, G., Crispo, B.: Internet of things: a survey on the security of IoT frameworks. J. Inf. Secur. Appl. **38**, 8–27 (2018)

2. Christin, D., Reinhardt, A., Mogre, P., Steinmetz, R.: Wireless sensor networks and the internet of things: selected challenges (2009)
3. Kocakulak, M., Butun, I.: An overview of wireless sensor networks towards internet of things. In: 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–6 (2017)
4. Raj, A., Steingart, D.: Review-power sources for the internet of things. J. Electrochem. Soc. **165** (2018)
5. Li, F., Xiong, P.: Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sens. J. **13**, 3677–3684 (2013)
6. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
7. Kanso, A., Ghebleh, M.: An efficient (t, n)-threshold secret image sharing scheme. Multimed. Tools Appl. **76**, 16369–16388 (2016)
8. Bao, L., Yi, S., Zhou, Y.: Combination of sharing matrix and image encryption for lossless (k, n) -secret image sharing. IEEE Trans. Image Process. **26**, 5618–5631 (2017)
9. Liu, Y.-X., Sun, Q.-D., Yang, C.-N.: (k, n) secret image sharing scheme capable of cheating detection. EURASIP J. Wirel. Commun. Netw. **2018**, 1–6 (2018)
10. Liu, Y.-X., Yang, C.-N.: Scalable secret image sharing scheme with essential shadows. Signal Process. Image Commun. **58**, 49–55 (2017)
11. Yan, X., Lu, Y., Liu, L.: A general progressive secret image sharing construction method. Signal Process. Image Commun. **71**, 66–75 (2019)
12. Guo, Y., Ma, Z., Zhao, M.-D.: Polynomial based progressive secret image sharing scheme with smaller shadow size. IEEE Access **7**, 73782–73789 (2019)
13. Yang, C.-N., Chu, Y.-Y.: A general (k, n) scalable secret image sharing scheme with the smooth scalability. J. Syst. Softw. **84**, 1726–1733 (2011)
14. Liu, Y., Yang, C.-N., Chou, Y.-S., Wu, S.-Y., Sun, Q.-D.: Progressive (k, n) secret image sharing scheme with meaningful shadow images by GEMD and RGEMD. J. Vis. Commun. Image Represent. **55**, 766–777 (2018)
15. Zhang, L., Zheng, X., Liu, Y.: Progressive secret image sharing scheme based on semantic segmentation. IEEE Access **8**, 173289–173297 (2020)
16. Zhang, L., et al.: Modular-based secret image sharing in internet of things: a global progressive-enabled approach. Concurrency and Computation: Practice and Experience (2020)
17. Thien, C.-C., Lin, J.-C.: Secret image sharing. Comput. Graph. **26**(5), 765–770 (2002)