Low Energy Interleaved Chaotic Secure Image Coding Scheme for Visual Sensor Networks Using Pascal’s Triangle Transform

G. SUSEELA¹, Y. ASNATH VICTY PHAMILA², G. NIRANJANA¹, KADIYALA RAMANA³, SAURABH SINGH⁴, AND BYUNGUN YOON⁴, (Senior Member, IEEE)

¹School of Computing Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu 603203, India
²School of Computing Science and Engineering, VIT University, Chennai Campus, Chennai, Tamil Nadu 600127, India
³Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences, Rajampet 516126, India
⁴Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea

Corresponding author: Saurabh Singh (saurabh89@dongguk.edu)

This work was supported by the Dongguk University Research Fund of 2021 (S-2021-G0001-00091).

ABSTRACT The resource-constrained camera integrated Visual Sensor Networks (VSN) have conquered numerous visual aided services from visual surveillance to habitat monitoring. VSN is capable of sensing, processing and communicating visual data wirelessly. These networks are built with inexpensive low power sensor motes with a lightweight processor, limited storage, and bandwidth. The huge amount of redundancy present in the images makes the processing and communication consume more energy than expected. The number of bits must be reduced using energy-efficient compression techniques for efficient transmission. Low computational energy and communication energy are always favored for an increased lifetime of the wireless sensor network. The highly sensitive and self-descriptive nature of images makes security in VSN even more critical. In this work, we propose an energy-efficient low bitrate secured image coder for resource-constrained VSN. Light weight design protocols are highly required in secured image transmission over VSN. Through this communication, we also propose a novel chaotic map using Pascal’s triangle. The system follows a unique interleaved fashion of compression and encryption process to consume less computational resources. A series of tests were carried out to validate the secured image coder’s ruggedness and its suitability in VSN. The performance and the strength of the low bitrate secured image coder are tested with compression efficiency and cryptanalysis tests. Simulations were carried out in Atmel’s ATmega128 processor for energy consumption analysis. The energy consumed by the proposed system for compression, encryption and transmission of an image of size $512 \times 512$ is 109.364mJ (milli Joules), which is only 4.57% of the energy consumed by raw image transmission. In addition, the system is implemented in real time image sensor platform based on Arduino Due board integrated with OV7670 camera module for real time verification and the experimental results validated the suitability of the indicated scheme in real time VSN.

INDEX TERMS VSN, low bitrate, secured image coding, chaotic map, image compression, encryption.

I. INTRODUCTION

The modern advancements in MEMS, CMOS hardware technologies embraced with communication technologies empowered image communication over low power Wireless Sensor Networks (WSN) and evolved as Visual Sensor Networks (VSN). Due to the significance of VSN, image communication has reached potential applications, including but not limited to habitat monitoring, critical infrastructure monitoring, surveillance, industrial control systems, smart home systems, traffic monitoring [1]–[3]. Besides, VSN is a resource-constrained system in terms of both hardware and power. Due to the volume of image data, low-power sensor nodes are more energy-constrained in processing
and transmitting the image data. Thus, to increase the network’s lifetime, the number of transmitted bits must be reduced using an energy-efficient image compression algorithm. Since VSN carry sensitive and self-descriptive visual data, attackers can inadvertently trap the images. Due to the resource-constrained nature of VSN, security is considered an optimally lower issue in VSN [4], [5]. As VSN are deployed in mission-critical applications, securing the image data is essential. Thus, both compression and encryption are equally essential in image communication. The complex scenario of energy-efficient secured image communication is addressed. Energy-efficient secured image communication is a focal need in VSN, as it aims to save the network resources and protect the sensitive image data. In this research work, a novel lightweight block-based chaotic image encryption is proposed. As energy-efficient integrated compression and encryption schemes are gaining more attention in saving the power consumption and securing image data of the VSN, the proposed lightweight image encryption system is integrated into the author’s recent work on energy-efficient image compression schemes developed for low power resource-constrained systems [6]. The image compression scheme proposed in [6] uses a integer based approximated Zonal binary DCT (Discrete Cosine Transform), floating point free quantization and dictionary less low memory coder dedicated designed for a resource constrained sensor node in VSN.

The rest of the paper is structured as follows; Section 2 presents the existing joint image compression encryption systems and their adaptability in VSN. Section 3 presents the existing image encryption algorithms in the VSN literature and the need for low complex image compression - encryption using interleaved processing. Section 4 describes the proposed chaotic image encryption using the Pascal triangle, and Section 5 proves its strength in securing the image data by various security measures. Section 6 presents the proposed brand new - state of art secure image coding system. The interleaved fashion of low-bitrate secured image compression and encryption and presents the energy consumption analysis’s experimental and simulation results. Section-7 presents the real-time implementation in Arduino Due platform. Section-8 concludes the paper with the summary and future work.

II. PRIOR WORKS ON JOINT IMAGE COMPRESSION AND ENCRYPTION SYSTEMS
The joint image compression and encryption systems are classified into three categories, according to the sequential order of processing i.e. (a) Compression before Encryption (CBE), (b) Encryption before Compression (EBC) systems, and (c) Simultaneous Compression Encryption systems (SCE). In EBC and CBE systems, compression and encryption are performed as two distinct stages of the secured compression. In SCE systems, the compression and encryption systems are fused as a single stage to emphasize simultaneous image compression and encryption.

A. COMPRESSION BEFORE ENCRYPTION SYSTEMS
Compression followed by encryption is better as data compression removes redundancy present in the image data. The compressed image will assume a more uniform distribution of pixels. Compression before encryption systems is intended to improve the compression performance in terms of coding efficiency. The image coding systems based on CBE will offload the computational complexity, and the storage requirement as encryption is done on the compressed image. However, the attacker may get clues about the secure coded image by various indications or hints that exist on it, for example, the size of the image. In the existing research works based on CBE, the compression efficiency was unfavorable [7]–[11]. Thus, the linearity exhibited in the integrating these two systems makes an attacker easily crack the cryptosystem without deliberating the compression scheme. Referring to Yuen and Wong et al., the work proposed under the category of CBE using DCT and SHA-1 had high key sensitivity and large key space to withstand brute force attacks but had poor compression performance [7]. Wang et al. proposed a solution for secured image coding based on chaotic map and arithmetic coding. In which encryption and compression are performed as two different stages, the adversary will fissure the encryption system regardless of the compression. On observing the NPCR values of this system, it is weaker against differential attacks also, the compression performance was inimical [8]. Some more research work can be addressed in the references [39]–[46].

B. ENCRYPTION BEFORE COMPRESSION SYSTEMS
In these systems, the encryption scheme is followed by compression [9]–[12]. The compression algorithms could alter the data fidelity present in the image. In order to preserve the fidelity of the data, encryption is performed before compression [13], [14]. Moreover, this category of systems focus is high on image encryption than compression efficiency. A recent work proposed by Zhou et al. has pointed out that the encryption before compression systems could not achieve high compression efficiency than the cutting-edge compression algorithms, which accept the plain image as input [12]. For resource-constrained VSN, energy-efficient computation is more stringent; acclimating encryption before compression is not viable [47]. Since in these systems, the entire pixel data of the image are processed by the encryption system, and most of them might be discarded by the compression system. The resources of the VSN will be exploited or overspent [48].

C. SIMULTANEOUS COMPRESSION AND ENCRYPTION SYSTEMS
The third classification of joint compression – encryption system is Simultaneous Compression and Encryption (SCE). The objective of SCE is to reduce the cost of secured compression [15], [16]. Zhau et al., under SCE,
used chaos theory and the Chinese remainder theorem [15]. It is found that the system could offer a compression ratio of 4:1 with decent randomness parameters such as entropy, correlation. However, it could not stand the known plain text attack due to simultaneous encryption and compression processing.

III. IMAGE ENCRYPTION IN VSN

This section discusses the image encryption systems principally designed for secured image transmission over VSN in the literature. Traditional encryption algorithms will encrypt the entire image, and the cost of encryption is generally high. Another encryption category is to encrypt only the part or portion of the image, which needs to be secured, known as partial or selective encryption. Due to the resource-deprived nature of the sensor networks, partial encryption or selective encryption algorithms attained scholars' focus in securing the multimedia content [4]. The partial encryption schemes offer a convincible level of security. Though the partial encryption systems seem energy efficient by decreased computational load, it requires additional computational resource for determining the sensitive portion of the image for encryption. These systems must appoint image analyzing tools such as but not limited to edge detector, foreground and background subtraction model [17], [18]. These tools also require an accountable amount of computational and network resources. Also the work proposed by Nandhini et al. [18], clearly states the challenge of video coding in VSN. They have used only five frames as video coding is expensive attempt in VSN. The joint compression and encryption systems could not offer both an efficient compression system and a strong cryptosystem.

Hence, an energy-efficient hybrid image coding scheme with a highly secured complete encryption system in which the compression and encryption systems are interleaved with low complexity and low energy consumption is aimed. Key features of the proposed system are

1) The full image encryption offered by the system assures strong security for the entire image content.
2) The proposed lightweight image encryption offers an average entropy of 7.9991, which ensures cryptosystem’s strength.
3) Independent block processing is adapted to suit the memory required of the Visual Sensor node.
4) The compression and encryption procedures are interleaved to consume less computational resources in resource-constrained VSN than sequential processing.
5) The total energy required by the proposed system, including interleaved compression-encryption, coding, and transmission over mica2 mote for a greyscale image of size 512 \times 512 is only 109.32mJ, which is as low as 4.57% of the energy required for the raw transmission.
6) The proposed system’s performance is evaluated in real-time using the Arduino Due board integrated with the OV7670 camera module.

A. CHALLENGES OF CHAOTIC BASED IMAGE ENCRYPTION IN VSN

Generally, chaotic systems require memory equivalent to a plain image’s size for assigning the pixels at their respective projected new positions without overwriting untreated pixels. Each pixel block should be read from the plain image and written into the new locations to accomplish the transformation. Then it must be read once again for further operations, which will consume more memory cycles, and hence energy consumption and latency due to memory access will be high. The transform must be complete before starting the diffusion and encoding process. Full frame processing by the lightweight processors present in VSN is not feasible. Thus, the chaotic-based image scrambling technique must be optimized to fit into resource-limited VSN. Simultaneously, the chaotic mixing scheme is attractive for VSN as they require only four multiplications, two additions, and two modulo-division per pixel block [19]. As VSN is enabled with the lightweight processor, chaotic encryption allows low memory implementation by independent block processing.

B. PASCAL TRIANGLE TRANSFORM

A novel chaotic transform called Pascal’s Triangle Transform (PTT) is introduced into the paradigm of image cryptography. The typical Pascal’s triangle is as depicted in Fig. 1. The power of Pascal’s Triangle is that it allows an image cryptologist with a vast number of patterns. These patterns are helpful as chaotic maps. (Can be employed as image scramblers for creating confusion). The basic Arnold transform and the generalized Arnold transform the secrecy of the system is concealed at the triangle’s levels. The chaotic transform map is generated by combining the first and second diagonal elements of level n and level n + 1 of the pascal triangle as given in the Eq. (1). Any 2 \times 2 matrix generated using Eq. (1) is unimodular. A square matrix’s unimodular property makes the transform matrix periodic and thus can be a good image scrambler [20].

\[
\begin{bmatrix}
    a \\
    b
\end{bmatrix}
= \begin{bmatrix}
    E_{ssl+1} & E_{ssl} \\
    E_{fft+1} & E_{fft}
\end{bmatrix}^{m} \begin{bmatrix}
    x \\
    y
\end{bmatrix} \mod N
\]  

where $E_{ssl}$ – the second element of the second diagonal of level n. $E_{fft}$ – First element of the first diagonal of level n. $(x,y)$ is the current pixel block position and $(a,b)$ is the projected point of the block(a,b). ‘m’ is the rotation key-value and N is the width of the image in blocks. PTT can produce an infinite number of transforms and produce various scrambling patterns.

C. PTT BASED IMAGE SCRAMBLING FOR RESOURCE-CONSTRAINED VSN

As VSNs are resource-limited, affording memory space equivalent to the image size is expensive, and full-frame processing is not feasible by the sensor node. To reduce the number of reads and writes and to reduce the additional space requirement, at first, the projected new position $(a,b)$
for the values \((x,y)\) is computed using Eq. (1). The pixel block at \((a,b)\) of the plain image read from the position \((a,b)\) and transferred for further processing without storing it in new space and transmitted as pixel block at \((x,y)\). Hence memory access and additional space requirement are significantly reduced. Each block is independently processed, and chaotic transform need not be complete. At the decryption, the pixel block position \((x,y)\) of the ciphered image is used to compute the original pixel block position \((a,b)\) of the plain image.

IV. PROPOSED LIGHTWEIGHT IMAGE ENCRYPTION USING PTT

The proposed block-based chaotic image encryption involves pixel block scrambling (confusion), pixel diffusion by bit rotations using hamming distance, and XOR operations with a diffusion matrix. The proposed image encryption system can be defined as Eq. (2).

\[
C = E(P, F, G) = E(P(l, m, N/n), F(C_1, C_2, C_3), G(a, b, w, z))
\]

(3)

where \(P(l, m, N/n)\) is the chaotic sequence generated by the PTT image scrambler. \(l\) is the level of pascal triangle, \(m\) is the rotation parameter, \(N\) is the width of the square image, and \(n\) is the pixel block size. The \(l\) and \(m\) are keys of the image scrambler. For an image of size \(512 \times 512\) the PTT with \(l = 2\) is periodic at the point \(m = 192\) i.e. at this point the scrambled image is the same as the plain image. The proposed system uses two levels of diffusion using the functions F and G, where F is the pixel diffusion function by three encryption keys \(C_1, C_2, C_3\). These keys are generated using Eq. (4) - Eq. (6). \(F(C_1, C_2, C_3)\) is computed as,

\[
C_1 = modulo\left(\sum (a, b) \times 256\right)
\]

(4)

\[
C_2 = \sum \sum \left[\frac{E_{\text{ssl}}+1}{E_{\text{gll}}+1}\left\{\frac{E_{\text{ssl}}}{E_{\text{gll}}}\right\}^m\mod 256\right]
\]

(5)

\[
C_3 = h_d(C_1, C_2)
\]

(6)

where \(h_d\) denotes hamming distance. The second level diffusion is emphasized using \(G(a, b, w, z)\). \(G\) generates a \(2 \times 2\) matrix using input pixel block position values \((a, b)\) and two other parameters \((w, z)\), the \(w\) and \(z\) are chosen as relative prime numbers. This step is required for strong sensitive to the input.

\[
g_{11} = (a^w + b) \mod 256 \text{ and } g_{12} = (b^w + a) \mod 256
\]

(7)

\[
g_{21} = (a^z + b) \mod 256 \text{ and } g_{22} = (b^z + a) \mod 256
\]

(8)

A. ENCRYPTION PROCEDURE

The original raw image is divided into \(n \times n\) small pixel blocks (where \(n\) can be 2 or 4 or 8). For illustration, the experiments were carried out for \(n = 2\) i.e. pixel block size is \(2 \times 2\).

1) The current pixel block position \((a, b)\) is computed by chaotic PTT using Eq. (1).
2) The pixel block \(X\) of size \(2 \times 2\) from the permuted block position \((a, b)\) is read.
3) The three keys \(C_1, C_2, C_3\) are generated using Eq. (4), (5), (6) respectively. \(C_3\) holds the Hamming distance between \(C_1\) and \(C_2\).
4) If the Hamming distance \(C_3\) is even, the pixel values of the block \(X_{(a,b)}\) is bitwise right rotated circularly by \(C_3\) times as

\(D1_X = \text{circular right shift (}X_{(a,b)} \ll C_3\)

Else if the hamming distance \(C_3\) is odd, the pixels are bitwise left rotated circularly by \(C_3\) times as

\(D1_X = \text{circular left shift (}X_{(a,b)} \gg C_3\)

5) A \(2 \times 2\) matrix is generated \(G_X = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix}\) using Eq. (7) and Eq. (8).
6) The second level diffusion is done through \(D2_x = G_X \oplus D1_X\) to deliver the ciphered pixel block.
7) The ciphered pixel block \(C_x = D2_x\)
8) Repeat step 1 to step 7 until all the pixel blocks are encrypted. The decryption process is the reverse process of encryption.
V. PERFORMANCE ANALYSIS OF THE LIGHT WEIGHT CHAOTIC IMAGE ENCRYPTION BASED ON PTT

This section debates the performance analysis of the proposed encryption system. Encryption and decryption outcomes of the test images of size 512 × 512 under Matlab are presented in Fig. 2 [21], [22].

A. SECURITY ANALYSIS

According to the theory of cryptology, an encryption system needs to be robust against various attacks [49]. The well-known attacks expected are statistical, differential, and brute-force attacks. Harshness to statistical attacks is assessed by histogram analysis and adjacent pixel...
correlation analysis [50]. A robust encryption algorithm should have more vital encryption keys. It is examined by key space and key sensitivity analysis for strong tolerance over brute-force attacks. The metrics, Number of Pixels Changing Rate (NPCR) and Unified Average Change in Intensity (UACI) measures the encryption system’s strength against differential attacks [23].

1) KEY SPACE ANALYSIS
The keys used in the proposed system are the parameters of chaotic scrambler and parameters of diffusion i.e., level ‘l’ of the PTT, the rotation parameter ‘m’, the four seed values of the PTT, the diffusion keys (a, b, w, z) of each pixel block. Suppose all the keys used in the proposed encryption algorithm are expected as 64-bit double-precision numbers based on IEEE floating-point standard with the precision of \(10^{15}\) [24]. The key space of the system reaches \(10^{150}\), which is approximately equivalent to \(2^{499}\). Considering the fastest computer that completes \(2^{80}\) computations per second is applied for brute force attacking the system and the number of seconds in a day is \(86400 (24 \times 60 \times 60)\). The time taken to complete the computational load may be calculated as,

\[
\frac{2^{499}}{86400 \times 2^{80} \times 365} \approx 10^{120} \text{ years} \quad (9)
\]

Thus, key space is very large enough for withstanding various kinds of brute-force attack.

2) KEY SENSITIVITY ANALYSIS
An encryption scheme should have high sensitivity encryption keys. A minimal change in the key values should result in a significantly great change in encrypted image [51]. This analysis number of tests was carried out with the change in encryption system’s various keys, like the rotation parameter ‘m’, by varying the parameter ‘l’ of PTT. The sensitivity analysis of Lena and Truck images is presented in Fig. 3. The key value ‘m’ is modified by one bit, and the encryption system offered a different image than the encrypted image by the correct key. The inability of the decrypted image to express any substantial useful information visually seen. Thus, the encryption system is highly sensitive to the changes in the encryption key.

3) STATISTICAL ANALYSIS
Shannon’s secrecy systems theory says an encryption scheme can be cracked by exploiting the statistical features present in the ciphered data [25]. A crypto-system should transmute the plain image into a pseudo-random encrypted image such that the correlation among the pixels should be below. The resistivity of the encryption system over statistical attacks is a vital factor in proving the crypto-system’s strength. Statistical tests, namely correlation analysis, and histogram analysis, are carried out.

The plain image is very well connected with the adjacent pixels as they convey meaningful information.
The encryption system’s role is to decorrelate the adjacent pixels well and avoid information leakage at statistical analysis [52]. This analysis is carried out by the random selection of 1024 pixels along with horizontal, diagonal, and vertical directions, respectively, from the plain and encrypted images separately.

\[
\text{corr} = \frac{\text{cov}(x, y)}{D(x) \times D(y)}
\] (10)

where

\[
\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))
\] (11)

\[
E(t) - \text{sample mean } E(t) = \frac{1}{N} \sum_{i=1}^{N} t_i
\] (12)

\[
D(t) = \frac{1}{N} \sum_{i=1}^{N} (t_i - E(t))^2
\] (13)

The correlation coefficient of these pixels of plain and encrypted images is computed using Eq. (10) and presented in Table 1. The correlation coefficient of plain images is closer to one due to the high association among the pixels. The correlation coefficient of encrypted images is closer to zero, which means that the pixels are highly decorrelated. A strong encryption system should offer a low correlation coefficient among adjacent pixels. The scatter plot of the correlation distribution of Lena’s plain and encrypted images is shown in Fig. 4. A regular distribution of the plain image’s correlation plots shows the existence of a strong correlation of pixels in the plain image. The dispersed distribution of the encrypted image intuitively shows the poor correlation among the adjacent pixels.

The histogram of the plain images and encrypted images is presented in Fig. 5. Also, Fig. 5 presents the histograms of two stages of the encryption scheme: pixel block scrambling, and diffusion. It is realized that the image scrambler does not generate any change in the grey levels, and the histogram of the permuted image is identified as the plain image [26]. The histograms of the encrypted images are flat, which means that the proposed system homogenizes the plain image and does not convey any useful information. The uniform distribution of the encrypted image is justified by Chi-square (\(\chi^2\)) test, and it is defined as

\[
\chi^2 = \sum_{i=1}^{2^8} \frac{(ob_i - ex_i)^2}{ex_i}
\] (14)

where \(ob_i\) and \(ex_i\) are observed and the expected number of occurrences of each of the 256 grey levels,
respectively. Considering 0.05 significance level $\chi^2_{(255,0.05)} = 293$ [27], the Chi-square value of the proposed system is 253, $\chi^2 = 253$. This infers that the pixel distribution of the encrypted image histogram is uniform as $\chi^2 < \chi^2_{(255,0.05)}$. Thus, the proposed system is strong against statistical attacks.

4) ENTROPY ANALYSIS

Shannon’s information theory, the entropy of a system emitting $2^n$ symbols with equal probability of occurrence is $n$. A strong encryption system must protect the plain images’s structural details and make the information content unpredictable. This unpredictability of an encryption system is determined by information entropy, and it is measured in bits. Since the entropy is computed for the full image, it is also referred to as Global Shannon Entropy (GSE) measure.

The entropy $H(s)$ is defined as

$$H(s) = - \sum_{n=0}^{255} p(n) \times \log p(n)$$

(15)

The ideal entropy measure for a greyscale image with $2^8$ grey levels is eight, and it is achieved when the histogram of the encrypted image is flat, i.e., all the grey levels are equally distributed. Entropy analysis results are presented under Table 2, and entropy is closer to 8 and higher than the existing systems. Thus, the proposed encryption system proves to be secured.

5) TOLERANCE AGAINST DIFFERENTIAL ATTACK

The attackers attempt to crack the security scheme by injecting small changes in the plain image and study the dependency between the ciphered images of the plain image before and after modification. The NPCR and UACI are the metrics used to measure resistivity against differential attacks. Let $S1$ and $S2$ are the encrypted images of the plain images $P1$ and $P2$, where $P1$ and $P2$ differ by only one-pixel modification. A binary matrix $BM$ equivalent to the size of the encrypted image is defined. The $BM(x, y)$ is assigned as 1, if $S1(x, y) = S2(x, y)$; if not, $BM(x, y)$ is assigned as 0. The NPCR and UACI are defined as,

$$NPCR = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} BM(x, y) \times 100}{M \times N}$$

(16)

$$UACI = \left[ \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} |s1(x, y) - s2(x, y)|}{255} \right] \times \frac{100}{M \times N}$$

(17)

| Image | Plain image [15] | Reference [14] | Proposed |
|-------|------------------|----------------|----------|
| Lena  | 7.44556757      | 7.997316061   | 7.997525484 | 7.99910782 |
| Barbara | 7.63211901 | 7.997485973 | 7.997492633 | 7.99905089 |
| Mandrill | 7.29254877 | 7.997369377 | 7.997455776 | 7.99915722 |
| Peppers | 7.57147256 | 7.9975376509 | 7.997503635 | 7.99914917 |

FIGURE 5. Histogram of (a) plain (b) permuted (c) encrypted images of Lena histogram of (d) plain (e) permuted (f) encrypted images of peppers.
The NPCR and UACI of various images are presented in Table 3. The ideal values of NPCR should be closer to 100%, and the values of UACI should be between 33%-36% for resisting the differential attack. From Table 3, it is found that the NPCR and UACI values are good and higher than the existing system. Thus, the proposed system can resist differential attacks.

**6) LOCAL SHANNON ENTROPY**

The Global Shannon Entropy is computed for the entire image, whereas the Local Shannon Entropy is computed for few pixel blocks of the ciphered image. It is accomplished by random selection of \( k \) disjoint pixel blocks of size \( q \times q \) of the ciphered image. The entropy is computed for \( k \) local blocks individually. The sample means of all the \( k \) local pixel blocks’ entropy is termed as Local Shannon Entropy (LSE) measure [28]. A sound encryption system must offer entropy closer to 8 for all the local pixel blocks. The LSE is computed as follows

\[
H_{LSE}(S) = \frac{1}{k} \sum_{i=1}^{k} H(S_i) \tag{18}
\]

The LSE analysis is carried out by randomly selecting seven-pixel blocks from PB1 to PB7 of the Peppers image’s encrypted image, as shown in Fig. 6a. From Fig. 6b, it is inferred that the entropy values of all the local pixel blocks are higher, and the local Shannon entropy measure is 7.9516. This proves that the proposed system offers high randomness at the block level also.

**7) ROBUSTNESS AGAINST NOISE AND DATA LOSS**

The encryption system must be resilient to noise and cropping attacks. Naturally, the image could be contaminated during transmission and processing. An encryption image contaminated by noise must preserve overall information content and convey some meaning at the decryption. If suppose the noise influences the encrypted image \( E_1 \) as,

\[
E_2 = E_1 + NWG \tag{19}
\]

where \( NWG \) is White Gaussian Noise and \( E_2 \) is noise added encrypted image [14]. The decrypted images of Lena, couple, and man are presented in Fig. 7. The decrypted images preserve the information content to certainty and visually recognizable.

- Further, the robustness of the encryption is studied against its sustainability against cropping attacks. The information loss or occlusion can momentarily affect the decrypted image. The cropping attack is carried out by 3.8% occlusion, and 0.9% occlusion of Lena and Truck images and the results are presented in Fig. 8. The decrypted images are visually good with very good

**FIGURE 6.** (a) Encrypted peppers image of size 256 \( \times \) 256, (b) Local Shannon entropy analysis plot with mean \( H_{\text{mean}}(s) = 7.9516 \).

**TABLE 3.** NPCR and UACI.

| Image   | Reference [14] | Proposed |
|---------|----------------|----------|
|         | NPCR (%)       | UACI (%) | NPCR (%) | UACI (%) |
| Lena    | 99.60          | 33.41    | 99.6208  | 33.55    |
| Cameraman | 99.61         | 33.40    | 99.6501  | 33.33    |
| Baboon  | 99.35          | 33.47    | 99.6078  | 33.59    |
| Boat    | 99.34          | 33.48    | 99.6140  | 33.67    |
FIGURE 7. Results of noise attack- decrypted images (a) Lena, (b) Couple, and (c) Man with white Gaussian noise with mean \( \mu = 0 \) and standard deviation \( \sigma = 0.01 \).

TABLE 4. Encryption quality.

| Image  | Reference [15] | AS/I | Reference [14] | Proposed |
|--------|----------------|------|----------------|----------|
| Lena   | 891.40         | 169.38 | 892.57         | 669.921875 |
| Airplane | 950.47     | 289.16 | 971.17         | 1806.492187 |
| Aerial  | 877.11         | 287.99 | 887.12         | 1030.015623 |
| Couple  | 884.00         | 223.86 | 925.61         | 819.703125  |
| Bridge  | 1153.3          | 141.32 | 1158.09        | 1559.046875 |
| Man     | 848.81         | 289.16 | 971.17         | 797.203125  |

PSNR suitable for Human Visual System (HVS). The proposed system’s chaotic PTT scrambler has decorrelated all the adjacent pixel blocks very well in the spatial domain. The pixel blocks in the occluded region are not contiguous blocks of the plain image. The cropping attack could not influence the system, and decrypted images are still meaningful with PSNR 27dB.

8) ENCRYPTION QUALITY

Encryption Quality is the deviation between the number of pixels of each grey level of the plain and the encrypted image. For a greyscale image with 256 grey levels, the \( EQ \) is computed as

\[
EQ = \frac{\sum_{g=0}^{255} |H_g(I) - H_g(IE)|}{256} \tag{20}
\]

where, \( I \) and \( IE \) are plain and the encrypted image respectively and \( H_g(I) \)-number of pixels in grey level \( g \). A significant variation in pixel intensities in between the plain and the encrypted image will offer superior \( EQ \). The Encryption Quality analysis results are shown in Table 4.

\( a: \) MEAN ABSOLUTE ERROR (MAE)

Mean Absolute Error is another measure to determine the performance of the encryption algorithm. It is computed as the absolute difference between the plain’s pixel values and the corresponding encrypted image.

\( b: \) MEAN SQUARE ERROR (MSE)

Mean Square Error is the cumulative squared difference between the original and the encrypted image. Higher MAE and MSE denote the more significant difference introduced by the encryption system from the plain image.

\[
MAE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} |IP(x, y) - IE(x, y)| \tag{21}
\]

\[
MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (IP(x, y) - IE(x, y))^2 \tag{22}
\]

where IP and IE are the plain and the encrypted image respectively. The MAE and MSE results are indicated in Table 5.

The encryption mechanism does not affect the reconstructed image’s quality when decrypted which means that the encryption system does not introduce any loss and offers a lossless ciphered image. Advanced Encryption Standard (AES) is a cipher, meaning that it is a method or process used to change raw information (usually human readable) into something that cannot be read. This part of the process is known as encryption. AES is implemented in software and hardware throughout the world to encrypt sensitive data. The AES (Advanced Encryption
VI. PROPOSED INTERLEAVED LOW BITRATE SECURE IMAGE CODING SYSTEM

In the proposed secure image coding system, the compression and the encryption schemes are combined in an interleaved fashion to attain computational efficiency and energy efficiency in VSN for forceful secured image encryption. The flow diagram of the proposed secured image coder is as shown in Fig. 9.

The author’s recent work on energy-efficient low memory transform-based image coder is employed for compression and entropy coding [6]. The SZBinary DCT is a variant of multiplier less fast integer DCT. It computes only the most significant components of size $2 \times 2$, i.e., DC, and the coefficients around the DCT matrix DC. The compression scheme’s adapted transform requires only 12 additions and 1-bit shift operations for an 8-point one-dimensional transform. Further, the transformed coefficients are quantized using bit shift operations by Q without the use of complex division operations, and the bitrate requirement decides the choice of Q value. The entropy coder used is a low complex low memory dictionary less complementary unary based coder.

The sensed raw image is divided into $8 \times 8$-pixel blocks. The processing chain of the proposed low bit rate interleaved secure image coder is as follows: Pixel block selection - Confusion - Transform- Quantization - Diffusion- Coding. Since the camera-integrated VSN node cannot afford the memory equivalent to the image’s memory size, the image is not scrambled at once entirely. Instead, the pixel block sequence of size $8 \times 8$ is read from the block position offered by the chaotic image scrambler is forward transformed by swift...
zonal binary DCT. The next element of the processing chain is diffusion. The diffusion is carried out in two stages to enhance security. Finally, the encrypted pixels are encoded using low memory listless coder presented in Ref. [6]. Modified enhanced complementary Golomb–Rice (MECGR) ensures low bitrate as it does not require any special code book or dictionary data structures which reduces the memory requirement significantly. It also ensures low power consumption as it does not require any special ordering. The confusion and diffusion are reversible, and these procedures are not introducing any information loss while ciphering the image. Thus, the confusion and diffusion stages are lossless, and the loss of information content is inclined only on compression stages of the proposed system.

**A. EXPERIMENTAL RESULTS AND PERFORMANCE DISCUSSION**

This section discusses the experimental set-up and the performance analysis of the proposed secured image coder. The low bitrate secured compression results of the standard greyscale test images of size $512 \times 512$ are presented in Fig. 10.

The compression performance is validated using bitrate, compression ratio, PSNR (Peak Signal to Noise Ratio), and SSIM (Structural Similarity Index Measure). The ruggedness of the lightweight encryption system is analyzed with statistical analysis and brute force attack analysis. The proposed system is exclusively designed for secure image transmission for resource-constrained VSN. Hence, energy consumption analysis at target platform Atmel’s ATmega 128 and CC1000 transceiver is also presented.

**B. SECURED COMPRESSION PERFORMANCE**

1) **BIT RATE (BR)**

It is defined as the minimum number of bits required for the coder to represent a pixel value and measured in bits per pixel (bpp). The proposed system offered 0.26bpp with acceptable image quality.

2) **COMPRESSION RATIO**

The ratio between the size of the original image and the size of the compressed image. The system offered a very high compression efficiency of 32:1.

3) **PEAK SIGNAL TO NOISE RATIO**

PSNR is the image quality assessment metric and measures the distortion in the processed image after applying image-processing algorithms.

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \quad (23)$$

-where MSE is the Mean Square Error.
4) STRUCTURAL SIMILARITY INDEX MEASURE
SSIM measures the similarity between the original image and the reconstructed image. SSIM is based on the human perceptual model. Fig. 10 results of proposed secured image compression of test images at BR = 0.26 bpp

$$SSIM(i, j) = \frac{2\mu_i\mu_j + K1}{\mu_i^2 + \mu_j^2 + K1} \cdot \frac{2\sigma_{ij} + K2}{\sigma_i^2 + \sigma_j^2 + K2}$$ (24)

where $\mu_i$ and $\mu_j$ are the sample means of plain image i and reconstructed image j, $\sigma_i$, $\sigma_j$ are the sample variances of i, j, and $\sigma_{ij}$ is the sample cross-covariance between i and j. The K1 and K2 will adjust the weak divisor’s effect and fixed K1 = 0.01 and K2 = 0.03.

C. ENERGY CONSUMPTION ANALYSIS
No work has been seen in the existing literature with energy consumption analysis of their image encryption system. The authors in this work have analyzed the energy consumption of the proposed lightweight secured image coder on the hardware platform. The mica2 sensor motes, built with Atmel’s ATmega128 processor, are considered for energy consumption analysis. The simulations were carried out for
TABLE 7. Energy consumption analysis for an 8 × 8-pixel block in Atmega128.

| Method               | Processing cycles | Total no. of Cycles | Code size (Bytes) | Processing time (ms) | Energy consumption (µJ) |
|----------------------|-------------------|---------------------|-------------------|----------------------|-------------------------|
|                      | Confusion | Compression | Diffusion | Coding |                      |                        |
| DCT(JPEG float)[34]  | -       | 824946      | -        | 21304 | 846450                | 21806                  | 105.85              | 2327.74             |
| Optimized JPEG [34]  | -       | 11060       | -        | 21304 | 18504                 | 18504                  | 4.08               | 89.81               |
| Proposed             | 225     | 1348        | 489      | 369   | 2635                  | 5810                   | 0.329              | 7.25                |

The energy required for transmission of the image for the raw transmission (E_{raw,tran}) of a greyscale image of size 512 × 512 is

\[
E_{raw,tran} = 8 \times 512 \times 512 \times E_s tran
\]  

\[
E_{raw,tran} = 2390.75 \mu J
\]  

An 8 × 8 - pixel block under AVR Studio 20060421 for measuring the energy consumption of the compression and encryption [32], [33]. AVR Studio is a tool for simulating Atmel’s microcontrollers developed by Atmel. The active power consumption of the ATmega128 processor is 22mW and, the clock frequency is 8MHz. The simulation is carried out by setting the AVR compiler with "O3" optimization, 8MHz clock frequency for ATmega128 processor, and the results are compared with JPEG (Joint Photographic Experts Group) standard and optimized JPEG [34] presented in Table 7.

The energy dissipation for transmitting a single bit (per bit) over the transceiver CC1000 radio of mica2 mote is computed by the Heinzelman model as done in [35]. Transmission energy per bit over the distance \(d\)

\[
E_{s,tran} = E_{elec} + \epsilon_d d^2, \quad d < d_0, \\
= E_{elec} + \epsilon_{amp} d^4, \quad d > d_0
\]  

The time taken to secure compress an 8 pixel was found to be 0.329 ms. Hence forth the proposed system offers a throughput of 194.25 pixels/ms.

VII. REAL-TIME IMAGE SENSOR BASED ON ARDUINO DUE WITH OV7670 CAMERA MODULE

An image sensor platform is designed by integrating Arduino Due with a low-cost OV7670 camera module [36]–[38]. The hardware setup is shown in Fig. 11. The raw image is captured by a low-cost camera module of resolution 320 × 240. Arduino does the image processing. Arduino offers great flexibility in the programming and development of embedded systems. The Arduino Due board is based on SAM3 × 8E Cortex M3 ARM-32-bit processor operating at 84MHz with SRAM 96KB. Arduino Due board is used in this work because of its larger SRAM size to meet image processing algorithms’ memory requirement among the various other Arduino boards. The other variants like Arduino UNO or Arduino MEGA boards require additional flash memory. The OV7670 is a CMOS VGA camera module operating at...
A low bitrate energy efficient secured image coder using a chaotic map based on Pascal’s triangle is presented. The encryption and compression procedures are interleaved for resource efficiency in low-power VSN. The system encrypts the full image and thus offers security to the entire information content of the image. The system offers a very high compression efficiency of 32:1 to satisfy the power and bandwidth constraint of the VSN. The statistical analysis and brute force attack analysis verified and validated the ruggedness of the encryption procedure. The total energy required by the entire system, including interleaved compression-encryption, coding, and transmission over mica2 mote for a greyscale image of size $512 \times 512$, is only 109.32mJ, which is as low as 4.57% of the energy required for the raw transmission. The proposed system consumes very little energy compared to raw transmission. The proposed system promises to incorporate a more robust image security system in image communication over resource-constrained VSN. The proposed system is also implemented in an image sensor platform built using Arduino Due and a low-cost OV7670 camera module for real-time verification. The real-time hardware implementation results have proven the suitability of the proposed system in a real-time environment. The research’s future scope is developing change detection systems and...
offering privacy protection in the real-time environment using multiple camera nodes.

REFERENCES

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, “Wireless multimedia sensor networks: A survey,” IEEE Wireless Commun., vol. 14, no. 4, pp. 39–45, Aug. 2007.

[2] Y. Lee, H. Ahn, H. Ahn, and S. Lee, “Visual object detection and tracking using analytical learning approach of validity level,” Intell. Automat. Soft Comput., vol. 25, no. 1, pp. 205–219, 2019.

[3] F. Stajano, N. Houlit, I. Wassell, P. Bennett, C. Middleton, and K. Soga, “Smart bridges, smart tunnels: Transforming wireless sensor networks from research prototypes into robust engineering infrastructure,” Ad Hoc Netw., vol. 8, pp. 872–888, Feb. 2010.

[4] D. D. O. Gonçalves and D. G. Costa, “A survey of image security in wireless sensor networks,” J. Imag., vol. 1, no. 1, pp. 4–30, 2015.

[5] D. Huang, P. Gu, H. Feng, Y. Lin, and L. Zheng, “Robust visual tracking models designs through kernelized correlation filters,” Intell. Automat. Soft Comput., vol. 26, no. 2, pp. 313–322, 2020.

[6] G. Suseela VOLUME 9, 2021 134591

[7] P. Li and K.-T. Lo, “Joint image compression and encryption based on discrete wavelet transform, chaotic maps and substitution box,” Signal Process., vol. 28, no. 6, pp. 670–680, Jul. 2013.

[8] B. Wang, X. Zheng, S. Zhou, C. Zhou, X. Wei, Q. Zhang, and C. Che, “Encrypting the compressed image by chaotic map and arithmetic coding,” Optik, vol. 125, no. 20, pp. 6117–6122, Oct. 2014.

[9] P. Li and K.-T. Lo, “Joint image compression and encryption based on alternating transforms with quality control,” in Proc. Vis. Commun. Image Process. (VCIP), Dec. 2015, pp. 1–4.

[10] C. Ge, J. Xia, and L. Fang, “Key-private identity-based proxy re-encryption,” Comput. Mater. Continua, vol. 63, no. 2, pp. 633–647, 2020.

[11] T. Xiang, J. Qu, and D. Xiao, “Joint SPIHT compression and selective encryption,” Appl. Soft Comput., vol. 11, no. 8, pp. 5092–5098, Dec. 2011.

[12] B. Wang, X. Zhou, C. Zhou, X. Wei, Q. Zhang, and C. Che, “Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 39–50, Jan. 2014.

[13] M. Kumar and A. Vaish, “An efficient encryption-then-compression technique for encrypted images using SVD,” Digit. Signal Process., vol. 60, pp. 81–89, Jan. 2017.

[14] M. B. El-Azouz and M. A. Gounden, “A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem,” Appl. Soft Comput., vol. 40, pp. 379–390, Mar. 2016.

[15] H. Zhu, C. Zhao, and Z. Xiang, “A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem,” Signal Process., Image Commun., vol. 28, no. 6, pp. 670–680, Jul. 2013.

[16] H. Hamdi, R. Rhouma, and S. Belghith, “A selective compression-encryption of images based on SPHIT coding and Chebyshev standard map,” Signal Process., vol. 131, pp. 514–526, Feb. 2017.

[17] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, “An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box,” J. Modern Opt., vol. 64, no. 5, pp. 531–540, Mar. 2017.

[18] S. A. Nandini and S. Radha, “Efficient compressed sensing-based security approach for video surveillance application in wireless multimedia sensor networks,” Comput. Elect. Eng., vol. 60, pp. 92–175, May 2017.

[19] C. Duran-Faundez, V. Lecuire, and F. Lepage, “Tiny block-size coding for energy-efficient image compression and communication in wireless camera sensor networks,” Signal Process., Image Commun., vol. 26, nos. 8–9, pp. 466–481, 2011.

[20] E. W. Weissstein. Unimodular Transformation. From MathWorld—A Wolfram Web Resource. Accessed: Nov. 3, 2019. [Online]. Available: http://mathworld.wolfram.com/UnimodularTransformation.html

[21] J. W. B. Z. Kominek. (1995). University of Waterloo. (Aug. 2017). [Online]. Available: https://links.uwaterloo.ca/Repository.html

[22] The USC-SIPI Image Database. Accessed: Dec. 9, 2019. [Online]. Available: https://sipl.usc.edu/database/database.php?volume=misc

[23] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutirrez, and C. Cruz-Hernández, “Suggested integral analysis for chaos-based image cryptosystems,” Entropy, vol. 21, no. 8, p. 815, Aug. 2019.

[24] IEEE Standard for Binary Floating-Point Arithmetic, IEEE Computer Society, ANSI/IEEE Standard 754, Aug. 1985, p. 754.

[25] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[26] D. Zhang and F. Zhang, “Chaotic encryption and decryption of JPEG image,” Optik, vol. 125, no. 2, pp. 717–720, Jan. 2014.

[27] H. S. Kwok and K. W. S. Tang, “A fast image system encryption based on chaotic maps with finite precision representation,” Chaos, Solitons Fractals, vol. 32, no. 4, pp. 1518–1529, May 2007.

[28] Y. Wu, Y. Zhou, G. Saveriades, S. Agaiaian, J. P. Noonan, and P. Natarajan, “Local Shannon entropy measure with statistical tests for image randomness,” Inf. Sci., vol. 222, pp. 323–342, Feb. 2013.

[29] W. Liu, K. Sun, and C. Zhu, “A fast image encryption algorithm based on chaotic maps,” Opt. Lasers Eng., vol. 84, pp. 26–36, Sep. 2016.

[30] X. Wang, X. Zhu, and Y. Zhang, “An image encryption algorithm based on Josephus traversing and mixed chaotic map,” IEEE Access, vol. 6, pp. 23733–23746, 2018.

[31] M. Gupta, K. K. Gupta, M. R. Khosravi, P. K. Shukla, S. Kautish, and A. Shankar, “An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things,” Wireless Pers. Commun., vol. 82, pp. 1–22, Aug. 2021.

[32] A. Shankar, et al. (1995). University of Waterloo. (Aug. 2017).

[33] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-Hernández, “Suggested integral analysis for chaos-based image cryptosystems,” Entropy, vol. 21, no. 8, p. 815, Aug. 2019.
G. SUSEELA received the B.E., M.Tech., and Ph.D. degrees in computer science and engineering. She is currently working as an Assistant Professor with the School of Computing, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India. She has 13 years of academic experience and four years of research experience. Her research interests include wireless image sensor networks, image-processing using deep learning, and network security. To her credit she has around 20 publications in various international journals.

Y. ASNATH VICTY PHAMILA received the M.E. and Ph.D. degrees in computer science and engineering from Anna University, India. She has around 16 years of academic and four years of industry experience. She has around 35 research articles to her credit. Her research interests include computer vision, wireless sensor networks, network security, and cyber physical systems. She also serves as a reviewer in reputed journals.

G. NIRANJANA received the B.E. degree from Madras University, and the M.Tech. and Ph.D. degrees in computer science and engineering from SRM University. She is having nearly 20 years of teaching experience. She is currently an Associate Professor with the Department of CSE, SRM Institute of Science and Technology. She has published around 20 scopus indexed articles. Her research interests include networking, machine learning, deep learning, and image processing. She has received the Young Investigator Award in 2012 and the IET Women Engineer Award in 2018.

KADIYALA RAMANA received the Bachelor of Technology degree in information technology from JNTUH, Hyderabad, India, the M.Tech. degree from Satyabhama University, Chennai, India, and the Ph.D. degree from SRM University, Chennai. He is currently working as an Associate Professor with the Department of Artificial Intelligence and Data Science, Annamacharya Institute of Technology and Sciences, Rajampet, India. He has 14 years of experience in teaching and research. He authored more than 20 international publications. His research interests include wireless sensor networks, software-defined networking with machine learning, and data analytics. He is an editorial board member and a reviewer of several journals of international repute.

SAURABH SINGH received the Ph.D. degree from Jeonbuk National University, Jeonju, South Korea, carrying out his research in the field of ubiquitous security. He was a Postdoctoral Researcher with Kunsan National University, South Korea. He is currently an Assistant Professor with Dongguk University, Seoul, South Korea. He has published many SCI/SCIE journal articles and conference papers. His research interests include blockchain technology, cloud computing and security, the IoT, deep learning, and cryptography. He received the Best Paper Award from KIPS and CUTE Conference, in 2016.

BYUNGUN YOON (Senior Member, IEEE) is currently a Professor with the Department of Industrial and Systems Engineering, Dongguk University. His theme of study has involved blockchain technology, patent analysis, new technology development methodology, and visualization algorithms. His current research interests include enhancing technology road mapping, research and development quality, and product designing with data mining techniques.

[48] J. H. Anajemba, T. Yue, C. Iwendi, P. Chatterjee, D. Ngabo, and W. S. Alnumay, “A secure multi-user privacy technique for wireless IoT networks using stochastic privacy optimization,” IEEE Internet Things J., early access, Jan. 11, 2021, doi: 10.1109/JIOT.2021.3050755.

[49] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, “A secured distributed detection system based on IPFS and blockchain for industrial image and video data security,” J. Parallel Distrib. Comput., vol. 152, pp. 128–143, Jun. 2021.

[50] H. Patel, R. D. Singh, R. G. Thippa, C. Iwendi, B. A. Kashif, and O. Jo, “A review on classification of imbalanced data for wireless sensor networks,” Int. J. Distrib. Sensor Netw., vol. 16, no. 4, Apr. 2020, Art. no. 1550147720916404.

[51] D. Datta, L. Garg, K. Srinivasan, A. Inoue, G. T. Reddy, M. P. K. Reddy, K. Ramesh, and N. Nasser, “An efficient sound and data steganography based secure authentication system,” Comput., Mater. Continua, vol. 67, no. 1, pp. 723–751, 2021.

[52] C. O. Iwendi and A. R. Allen, “Enhanced security technique for wireless sensor network nodes,” in Proc. IET Conf. Wireless Sensor Syst. (WSS), Jun. 2012, pp. 1–5.