Efficient and Secure Visual Data Transmission Approach for Wireless Multimedia Sensor Networks

A. Mostefaoui
FEMTO-St Institute DISC dep.
University of Franche Comte
Belfort, 90000, France
Email: ahmed.mostefaoui@univ-fcomte.fr

H. Noura
CEA Grenoble
17 Rue des Martyrs, 38000 Grenoble
Email: hassan.noura@gmail.com

Z. Fawaz
FEMTO-St Institute DISC dep.
University of Franche Comte
Belfort, 90000, France
Email: Zeinab.fawaz@femto-st.fr

***Abstract*—Wireless Multimedia Sensor Networks (WMSNs) have to deal with two main opposite constraints: (a) the voluminous nature of the sensed data, almost of megabytes order on one hand and (b) the limited resources, characterizing specifically WMSNs platforms (limited energy provision and CPU power, wireless communications, etc.) on the other hand. Additionally, as these platforms are open infrastructures, they are hence vulnerable to several types of attacks. In this paper, we propose a new and novel approach, specifically tailored to significantly reduce the transmitted multimedia data whilst allowing a high level of security, in particular data confidentiality. In fact, rather than using traditional cryptography systems which applied on multimedia data, inquiring a huge communication and hence overhead hence are not suitable within WMSNs, our approach begins first by transforming the input images using Voronoi tessellation, that reduces significantly their volume while preserving at the same time their perceived quality. As this transformation is performed on a random fashion basis, this randomness ensures then the content confidentiality. The proposed approach achieves hence both : (a) reducing noticeably the amount of the data sent by the source nodes, prolonging hence the overall network lifetime and (b) makes the network more robust against attacks. We study the parameters for setting up our approach by incorporating two schemes (basic one and more elaborated one). Finally, we demonstrate, through extensive experiments, the robustness (i.e., secure against several types of attacks) and the effectiveness of our approaches over the current state-of-the-art techniques.**

I. Introduction

Recent years have witnessed huge advances in multimedia device miniaturization as well as in wireless communication performance. The availability of cheaper hardware as CMOS cameras and microphones has emerged the development of large scale Wireless Multimedia Sensor Networks (WMSNs) [1]. In such a network, each sensor is able to capture, process and deliver multimedia data (mainly still images) over wireless connections. The targeted applications of WMSN are numerous, ranging from large military multimedia surveillance applications to automated assistance for the elderly persons, including advanced health care applications, home automation systems, etc. Many of these applications raise new theoretical and practical challenges on the design and the development of WMSNs. In fact, multimedia data are intrinsically different from traditional scalar data in the sense that they are very voluminous and their delivery is usually time sensitive (real-time constraint). These characteristics impose several requirements on the deployment of WMSNs as: (a) the availability of a large communication bandwidth in order to support multimedia streams, (b) the supply of additional CPU capabilities to sensors to be able to process multimedia data, (c) the development of new multimedia data transmission algorithms with the aim of reducing the overall network load, (d) and more importantly, the ability of securing the transmitted data since WMSNs are open infrastructures and consequently are very vulnerable to attacks. In addition, as commonly known, nodes in WMSNs have limited energy provision, as they are driven by batteries. Managing node's energy remains hence the main concern when designing and deploying large scale WMSNs, especially when dealing with voluminous data. Hence, reducing the transmitted data between nodes will be considered as the major goal of any technique in order to prolong the network lifetime, as communications, in particular transmissions, remain the most energy consuming tasks [1]. However, traditional cryptographic approaches for multimedia data usually add additional data in order to secure the content (i.e., steganographic approaches for instance). By doing so, they also contribute to shorten the network lifetime. Obviously, in such approaches, there are trade-off between the security and the network lifetime.

These antagonistic requirements (i.e., preserving node's energy, transmitting voluminous data and securing them) motivate the need for the development of **integrated approaches** that could handle all these requirements at once.

In this paper, we propose a novel integrated approach that mainly focuses on reducing the amount of multimedia data sent from the source sensors to the sink while securing them. In other words, instead of separating the two processes; i.e., reducing the data volume and securing them, we propose a new approach that merges these two steps into one step.

A. Motivations

Let us consider a real wild monitoring application example, in which a group of visual sensors are deployed to detect animals and communicate their locations to the base station (e.g., *Sink*). In such an application, each source node captures periodically, at a specified rate, an image and sends it to the sink, through multi-hop communications. In order to reduce

the amount of data to be sent, compression techniques, such as the standard JPEG [2], are usually used. Recent research works have also addressed the issue of image content confidentiality together with image compression [3]. Nevertheless, the amount of data remains voluminous, which is still a strong assumption for WMSN platforms. Other research works have focused on the content of frames i.e., instead of sending the whole frames, only detected objects of interest are sent by the nodes [4]. Nevertheless, these approaches necessitate powerful processors and large memories, which are far to be met by current WMSNs platforms.

Ideally, we are looking for an approach that could satisfy the three main constraints: (a) reducing the amount of data without altering the semantic of the content (i.e., the content will always be comprehensible by the sink), (b) ensuring the confidentiality of the transmitted data without incurring communication overhead and (c) exhibit low complexity in order to be handled by limited devices as those of WMSNs.

Obviously, there is a trade-off between these three antagonistic objectives and we believe that the target application can play an important role in finding a good trade-off. For instance, in our running application, if we consider that the main objective is to "recognize" the detected animals, it is hence worth to send data for that objective. In other words, the sink will not be interested in high definition images but images allowing the recognition of the observed animals. For instance, in Figure 1, we present two versions of the same image representing a tigger: the left one is a JPEG image and the right one results from our approach. We can see clearly that the content of the image is still recognizable, even thought the second one is a bit degraded. However, what is important from the network point of view, is that the second image necessitates only 1% of the total amount of data to be sent, in comparison to the first one. In other words, the second image *saves 99% of the network transmissions*.

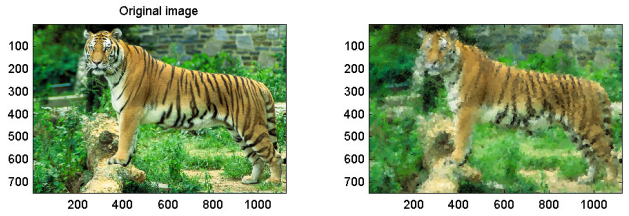


Fig. 1: Two different quality of the same image: the left one is a JPEG image, whereas the right one results from our approach. To reconstruct the right image, our approach necessitates only 1% of the total data of the left one.

Besides to this huge reduction of the transmitted data, which significantly prolongs the network lifetime, our approach also ensures content confidentiality and fulfills the applications requirements in terms of image quality.

B. Contributions

To the best of our knowledge, this is the first integrated approach, tailored for both data reduction and content confidentiality preservation, with regards to the intrinsic limitations of WMSNs platforms. The key idea behind our proposal is the use of Voronoi tessellation to represent the transmitted image. Hereafter, we highlight its different steps: first, the Voronoi tesselation is constructed by using a predefined number of points (noted N), each of which with its coordinates (x and y) within the original image. These points are uniformly generated by a random number generator. The source node sends then these points to the receiver, which in turn is able to reconstruct the image by following the reverse process i.e., generating N points using the same generator as the source node and reconstructing then the image. This process is secured by keeping secret the random number generator (with the assumption that this generator generates always the same sequence of number).

Our approach exhibits a very low time complexity, since it involves Voronoi tessellation process which has $O(N \times log(N))$ time complexity. This makes our proposal well suitable for WMSNs limited platforms.

Even though this basic approach could fulfill the requirements of a large brand of WMSNs application, it still suffers some security vulnerabilities, in particular the assumption about the secret random number generator. In fact, in this approach, all source nodes and the sink use the same random number generator. If, for any reason, the random sequence has been discovered by the attackers, the whole system will be then compromised. This basic approach is somehow static in the sense that the random number generator is fixed for all.

To overcome this drawback, we provide in the paper, an enforced version of our approach by integrating a dynamic mechanism to constantly change the random sequence. We validate the performance effectiveness of our approach through experiments and we provide theoretical results demonstrating its robustness against several types of attacks.

The remaining of the paper is as follows: (a) Section II provides the related work. In Section III, we present the first approach, called *Basic Approach*, and we also provide its performance and security analysis. The following section (e.g., Section IV) presents a more enhanced approach; e.g., *Dynamic Approach*, that overcomes the weaknesses of the basic approach. The two proposed techniques are evaluated and the results are discussed in Section V. In Sections VI and VII, we discuss the security features of dynamic approach. Finally, Section VIII concludes the paper.

II. Related Work

A. Security in WSN

Security issues in WSNs have attracted many research works because of the numerous hardware limitations characterizing them [1]. First, addressing security aspects starts by ensuring a secure way for key exchange. For that reason, several key establishment schemes are proposed, beginning

by Symmetric key cryptography as in [5], where a single shared key is used between the two communicating parties. In the context of WSNs, several pre-distribution random keys are proposed [6], [5], [7], [8]. In [5], a large scale sensor network connectivity is presented, where a distribution of a key ring between each participating node within the sensor network is performed, with the fact that the key ring is a random number chosen randomly from a set of keys before deployment. Then, any two nodes sharing the same key can communicate with each other. Furthermore, an enhancement of this approach by using multiple key re-distribution is explained in [9]. Also, another approach, based on the introduction of a third trusted common party between each two communicating nodes is described in [10], in a way that any communication between two nodes A and B is fulfilled throughout a third node C that shares the same key with both nodes. Later on, due to the fact that a sensor node consumes less energy and requires less computational power compared to the Base station (BS), a hybrid key establishment between the sensor node and the Base station (BS) is investigated in [11]. So, all cryptographical aspects are verified on the BS, and an authentication approach based on the use of Elliptic Curve Cryptography (ECC), characterized by its small key length, is performed between the BS and the requested sensor node. The use of symmetric key demonstrates its success for applications with low computational complexity, but a major common problem of this approach is that the single shared key must be commonly known by the two communicating parties before establishing the secure communication, in addition to the huge memory size needed to store all the keys.

These drawbacks motivate the researchers to use the alternative public key algorithms in the realm of WSNs, where two different keys are used: one is made public and the other is kept private. In [12], Harstein et al successed in the implementation of public key cryptography in WSNs by using two hardware's: Rabin and NetruEncrypt hardware that proved its energy and power efficiency. Next, in [13], Watro et al focused on ensuring the confidentiality, by implementing a TinyPk security scheme that is based on the use of RSA cryptosystem with e=3 (as public exponent) and assuring the source authentication by using a Diffie-Hellman key exchange. the problem with asymmetric key is that it is typically too computationally expensive for the individuals nodes in a sensor network, but this argument is not true for all cases, as in the proposed schemes in [12], [14], [13] that showed that public key cryptography is adequate to be used in very constrained environments.

B. Security in WMSN

Security in WMSNs is still a new and hot research topic [1]. The main purpose of a sensor node in WMSNs is to handle visual data that have higher constraints in terms of processing power, buffering, bandwidth, etc. In [1], an analysis and study of security aspects and requirements that must be respected in the design of a WMSN is explored. Among these requirements, privacy is considered as crucial issue in many applications that run under WMSN. We distinguish two different types of privacy protection and masking against attacks: (i) The first type, is privacy aware mechanism based on data cloaking, that aims to hide the message contents by applying a perturbation technique on data using specific patterns as in [15] where a new method for ensuring the integrity and confidentiality using distributed approach is discussed. (ii) The second type of privacy is the privacy policy as in [16] where the transmitted data has a special type and it will be received by a specific users under some conditions. Another study for improving privacy is presented in [17], where a privacy buffer is used to prevent access to specific data and then remove personal identifiable information. In [15], a distributed privacy paradigm, that operates in decentralized manner, is discussed. In this approach, each visual sensor V_i, in a cluster, computes a share value U_i from its observation, and send it to the BS. The BS receives all shares U_i coming from different paths, and hence is able to reconstruct the initial observation. Noting that, this scheme ensures the security against eavesdropping and tampering attacks, so if an attacker has access to one share value, he can not deduce others transmitted information. But, on the other side, it does not ensure data confidentiality, since each share value is transmitted in a disjoint path to the BS.

Also, another field that gain the attention of researchers is the use of Free-Space Optical (FSO) sensors in WMSNs, due to their higher achievable bandwidth, lower power consumption and smaller size. FSO is based on a light of sight (LSO) unidirectional communication, that transmits light beams signals (laser and diodes) and achieves a higher data rate in a few kilometers. In this context, a secure routing protocol OPSENET is discussed in [15], with ensuring a BS-circuit discovery, source authentication as well as integrity of routing systems. OPSENET overcomes the black-hole and sinkhole attacks by establishing the global picture of the network at the Base-station (BS), with identification of the location information. Moreover, it reduces the energy consumption and minimized the computational overhead by combining broadcasting and data gathering into one step. On the other side, using FSO technology in the realm of WMSNs is still an open research due to some atmospheric conditions such as fog, rain, and heavy snow, that render the network useless. In addition to solar interference that occurred when an outside light source (sunlight) intercepts in the transmission process, and affects the whole system.

It is noted that all existing approaches, including both: schemes that are provided to overcome security problems, and that are proposed to solve data distribution issue in WMSNs, suffer from many problems such as lack of confidentiality, vulnerabilities against attacks, and low performance. In this paper, we propose a new scheme, based on Voronoi tessellation, that fulfill in one step: the security requirements, data reduction and low computational complexity.

III. Basic Approach

In this section, we present, through a running example (Lena image), the different steps of our approach from image acqui-

sition by the source node until its reception and reconstruction by the sink.

A. Voronoi Tesselation

The Voronoi Diagram (VD) of a set of points in the plane is a tessellation that divides the latter into convex polygons, called Voronoi cells. Each cell corresponds to a point, also known as a site, and is the locus of all points that are closer to this site than to the others. Figure 2, shows an example of a Veronoi tessellation.

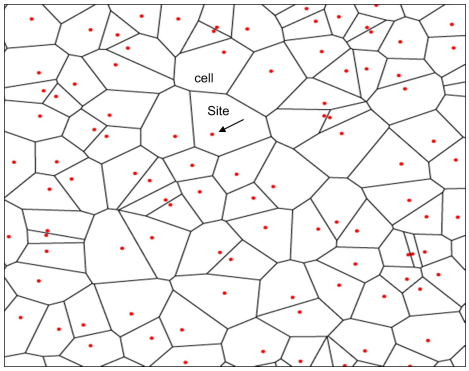


Fig. 2: Voronoi Tessellation: sites (e.g., points) and their related cells.

B. Source Nodes

In our approach, each source node, after image acquisition, applies the Voronoi tessellation on this input, by generating N random sites that are uniformly distributed within the image dimensions. Then, for each cell, we compute the mean color of all pixels belonging to it. This will be the color of the cell. Finally, the image is represented by a vector containing all the colors of the Voronoi cells. Figure 3 shows the different steps of this transformation.

Fig. 3: Input image transformation at the source node, through Voronoi tessellation: (a) original image, (b) Voronoi tessellation and (c) cells mean color computation.

It has to be noted the impact of the number of sites (e.g., N) on the quality of the resulted image. In fact, high number of sites result to a better image quality and *vice-versa*. This parameter must be studied in function of the target application quality requirement and fixed accordingly. We also note that this parameter is not fixed for all and could adapted dynamically with regard to the instantaneous requirement of the application. For instance, if an event of major importance has been detected and the sink is willing a higher quality, it could then ask the source node to increase the number of sites. Inversely, in order to preserve the network resources, the sink could also control the quality by decreasing the number of sites. In this sense, our approach offers a complete control to the sink on the quality of the received data. We have studied the impact of this parameter in our experiments presented in Section V.

Once the color vector of sites has been constructed in the same order as the random sites sequence. The source node sends then this vector to the sink.

C. Sink

Upon receiving the vector color from the source node, the sink will proceed in the reverse process as the source node. We assume that they share the same random number generator with the following characteristic:

Assumption 1: the source nodes and the sink have the same random number generator which generates always the same sequence of numbers.

Hence, the sink generates the same Voronoi tessellation and then is able to reconstruct the image from the received color vector. The overall process diagram is presented in Figure 4.

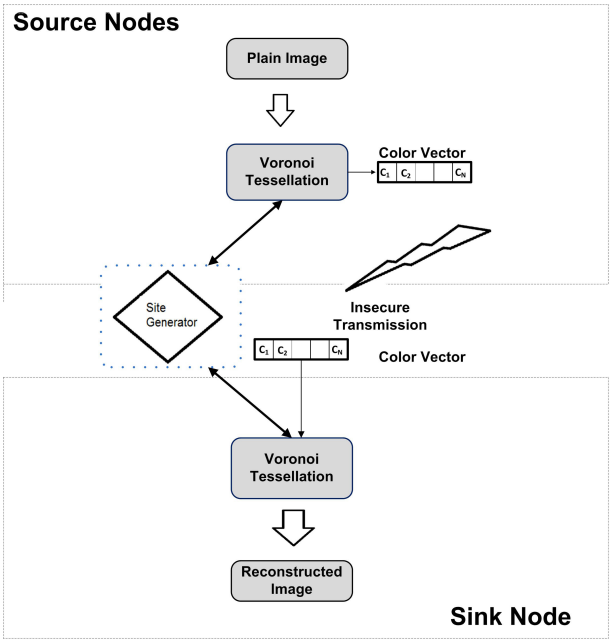


Fig. 4: Functional diagram of the source nodes and of the sink.

D. Performance and Security Analysis

The basic approach could be seen as a *fixed secret key approach*, in which the sites generator is kept secret between the sources nodes and the sink. Such a generator could be implemented in a hardware manner, on the concerned nodes in order to gain in performance. In the same manner, previous works [18] have shown that Voronoi tessellation process could be implemented in $O(Nlog(N))$, where N stands for the

number of sites, and does not necessitate large memories. *In fine*, our basic approach is very effective for limited devices platforms.

From security point of view, it represents however several vulnerabilities, mainly due to the fact that the secret key is **static**. Indeed, the latter is fixed for the whole network lifetime and consequently does not change over the time. Hence, once the random sequence is cryptanalyzed and discovered by the attacker, the whole systems is then compromised for the rest of its lifetime and could not be secured again. In other words, the content confidentiality is not ensured any more.

Even it is not easy to cryptanalyze such a system, because it relies on the content of images. Hence, static secret key represents nevertheless a serious vulnerability to the system. For this reason, we investigate a another approach in which the secret key is dynamic and change for every input image.

IV. Dynamic Approach

For enhancing security and reducing the cryptanalysis attacks, **Dynamic** key approach is used in our scheme instead of static key approach to ensure data integrity and confidentiality.

The importance of using a dynamic key is demonstrated by this situation: if an attacker gain access to the sites generator that is shared secretly between the sensor nodes and the sink, and succeeds to extract such random sequence, all others sequences in the system are still secure, since they are encrypted using different keys, and hence the whole system is not broken.

In this section, the three types of keys used in our approach is discussed. First, the re-initialization of the master key denoted by MK_{c1} is explained. Then, the generation of Session key SK_{c1} for each master key is discussed. And finally, the generation of the Dynamic key $DK_{c1,c2}$ from the session key is investigated.

1) Master Key Generation: A secret key is first agreed between the sensor nodes and the sink for a period of time designed the time taken to execute W number of images (in our approach, we set W=111 images). This private key called 'Master Key' and it is designed by MK_{c1}, where $c1$ is a counter that is incremented after the execution of W images.

2) Session Key Generation: Within the period of execution of W images, we generate from the Master key, a new key called 'Session Key' by concatenating the Master key MK_{c1} together with the counter $c1$, and the address of the source node denoted by $addin$. This concatenated form is then hashed using the hash function $SHA-512$ [19], to perform at the end, the session key corresponding to this MK_{c1} key.

Each session key SK_{c1} is used to execute a specified d number of images represented by a counter $c2$, where $d \leq W$ (Here, we take d=37 images). So, from each Master, we generate three session keys

3) Dynamic Key Generation: The session key value SK_{c1} is Xored with the initialization vector IV to perform X_{c1}. This resultant value is latter concatenated with the $c1$ value and the address of the source node $addin$. Those, are used as the input of the hash function process using $SHA-512$, to perform an output called V_{c1}. Finally, a dynamic key denoted by $DK_{c1,c2}$ is generated for each session key, by hashing the concatenated form $(V_{c1}||c1||c2||addin)$ using $SHA-512$.

This technique overcome the fixed key problem, and prevent an attacker that gain access to such random sequence to compromise the whole system. Noting that, the Master key MK_{c1}, the Session key SK_{c1} , Dynamic key $DK_{c1,c2}$ and the IV have the same key size which can be 128, 256, or 512 bits.

A pseudo-code for the dynamic key generation is well explained in Figure 5.

```
1:  procedure KEY_UPDATE(MK, IV, adin, i, j, c1, c2)
2:      if i ≥ w then
3:          c1 ← c1 + 1
4:          SK_c1 ← SHA_512(MK||c1||adin)
5:      else
6:          if j ≥ d then
7:              X_c1 ← SK_c1 ⊕ IV
8:              V_c1 ← SHA_512(X_c1||adin||c1)
9:              c2 ← c2 + 1
10:             DK_c1,c2 ← SHA_512(V_c1||adin||c1||c2)
11:         end if
12:     end if
13:     return DK_c1,c2, SK_c1, c1, c2
14: end procedure
```

Fig. 5: Key update's algorithm

A. Dependent-Key Point Selection

A binary additive stream cipher RC4 is used to generate a keystream from each dynamic key $DK_{c1,c2}$. RC4 is chosen to be used in our approach within the process of dynamic-key-generation due to its fastness and lower computational complexity (complexity equal to O(n) where n is the size of the plaintext). RC4 is parametrized by its block size n and consists of a table of size 2^n words that is known as S-box, and used to perform the permutation technique [20], in addition to the two counters i and j that are used in the swap operation. So, the dynamic key $DK_{c1,c2}$ is used as an input of the RC4 scheme with key length denoted by l bytes (key size in bits can be 128, 256, or 512). Then, the S-box is used to perform the permutation process followed by a swap operation using the two counters i and j to produce at the end the key-dependent value denoted by the keystream z.

The output z is the keystream of the RC4 function, and its value change for every dynamic key. Finally, each two bytes of the resultant output z are used to represent a unique point with coordinates x and y . These different new coordinates (x and y) are used to construct the Voronoi tessellation of the image.

B. Source Node

In the proposed scheme, the set of coordinates (x,y) generated from the keystream are used to construct the Voronoi tesselation of the image. Then, for each Voronoi cell, the color of this cell is calculated as the mean of all pixels belonging to it. After calculation the color for all Voronoi cells, the color values are stored in a vector called "color vector", which is transmitted through intermediate nodes, to reach the sink node.

It seems that the reconstruction of the input image at intermediate nodes is highly difficult, since intermediate nodes have no knowledge about the dynamic key sequence that is used to perform the Voronoi tessellation, and they only have information about the color vector without any previous knowledge about the set of coordinates (x, y). Hence, intermediate nodes are only responsible on the transmission of the color vector from the source node to the sink, and all coordinates (x, y) remain hidden during the transmission process. This secure, low complexity and efficient transmission facilitate the real deployment of the proposed scheme within WMSNs based applications, where the related platforms are characterized by its limited resources.

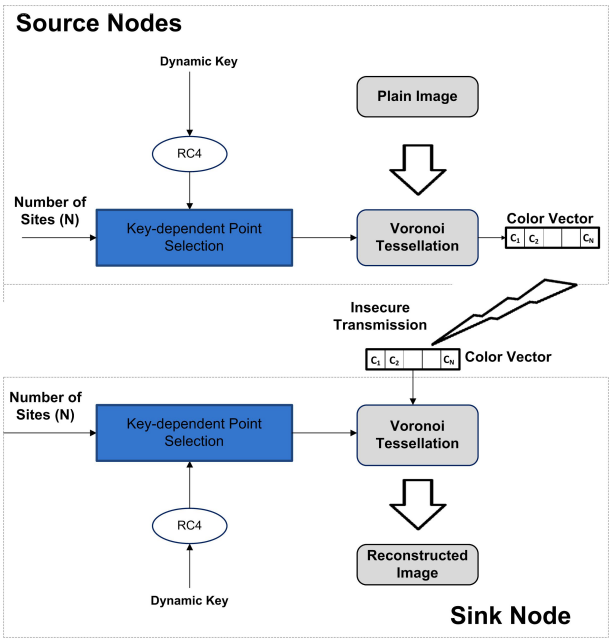


Fig. 6: Functional diagram of the source nodes and of the sink in the Dynamic Approach.

C. Sink

At receiver side, the reconstruction of the original image content is performed by applying the same techniques that are applied at the source node. This reconstruction necessitates two techniques : the regeneration of the dynamic key and the Key-dependent Point Selection. The different steps of the this reconstruction scheme are illustrated in Figure 6, and discussed as following:

1) Dynamic Key Regeneration: Actually, each point with coordinates (x, y) is derived from a keystream (output of the $RC4$ stream cipher).
A regeneration of the same dynamic key sequence is recommended first, in order to reconstruct the same Voronoi tessellation. For that reason, from the Master Key MK_{c1} that was shared secretly between the source node and the sink before information exchange, the receiver builds the session key SK_{c1}, then the dynamic key $DK_{c1,c2}$ using the same procedure that was applied at the emitter side.
After that, the $RC4$ stream cipher is applied on the generated dynamic key $DK_{c1,c2}$ to obtain the keystream z. When, this step is performed correctly, the receiver can use the sequence of keystream z to rebuild the same set of points used by the source node, and hence to reconstruct the whole input image.

2) Dependent-Key Point Selection: After regeneration of dynamic keys $DK_{c1,c2}$ sequence, and keystreams sequence denoted by z, each two bytes of the z sequence represents a point with coordinates (x, y). Then, from the set of (x, y) coordinates, we build the Voronoi tesselation, taking into consideration that the color for each Voronoi cell is represented by one component of the received color vector.
By that, a reconstruction of the original input image is realized successfully, using techniques that didn't require a high complexity.

V. Performance Evaluation

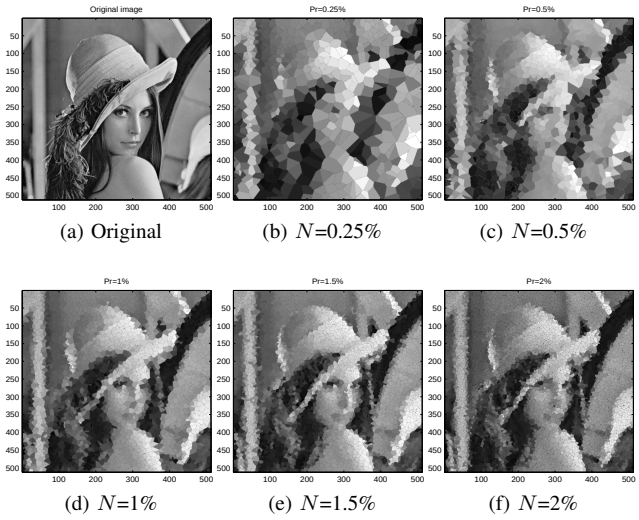
In this section, we report on the performance evaluation of our proposed schemes and discuss their cryptographic properties. More precisely, this cipher is subjected to several statistical tests such as uniformity, randomness, and key sensitivity to assess its efficiency and consistency with security standards.

Before diving into security details, we first study the impact of the parameter N (i.e., number of Voronoi sites) on the quality of the resulted image.

A. Number of Voronoi sites

For this series of experiments, we have considered the well known Lena image (512×512 pixels) in gray scale as an input image for our approach. We have then varied the number of Voronoi sites, in percent of the number of pixels. The resulted images are then compared, in term of their perceived quality, to the original one by using the Structural Similarity index SSIM [4], [21], [22](normalized value between 0 and 1) which is a reference metric used to measure the similarities between two images. We used this index instead of the more widespread Peak Signal to Noise Ratio (PSNR), and Mean squared error (MSE), because the latter have been shown its inconsistency with human eye perception [4], [21], [22]. Figure 7 shows examples of resulted images for different values of N (e.g., 0.25%, 0.5%, 1%, 1.5% and 2%).

For each value of N, the corresponding SSIM value is the average of 1000 runs of the same voronoi tessellation. The results are presented in Figure 8. We can observe that, for a value of $N \geq 1\%$, a SSIM index value of 0.7 is attained,



(a) Original (b) N=0.25% (c) N=0.5%

(d) N=1% (e) N=1.5% (f) N=2%

Fig. 7: Impact of the Voronoi sites number on the generated images.

which means that the visual content of the image is apparent and comprehensible [4]. For higher values of N (i.e., beyond 3.5%), SSIM index does not change significantly. However, for lower values of N (less than 1%), SSIM index remains small. As verified in the images of Figure 7, for $N = 0.25\%$ for instance, the image is still not clear. As a result, we conclude that $N = 1\%$ represents a good compromise value between perceived quality of the transmitted image and its size.

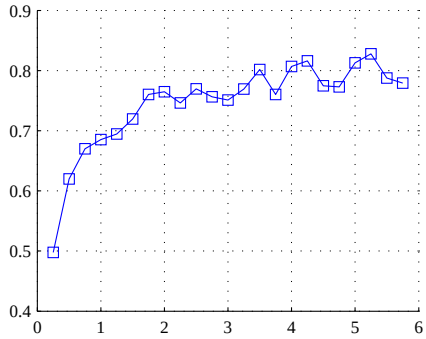
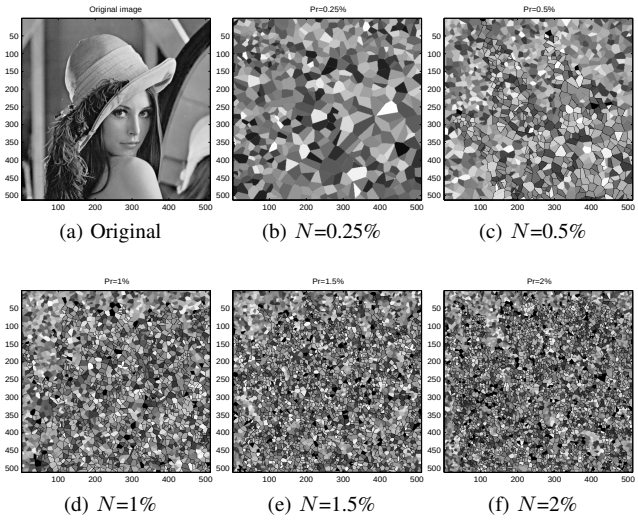


Fig. 8: SSIM index variation in function of the number of Voronoi sites (%).

From performance point of view, our proposal can hence save 99% of the network resources, mainly communications which are known to be the most energy consuming tasks in WMSNs [1], in comparison with other approaches that are based on the whole frame transmission. Thus, with ensuring at the same time the confidentiality of the transmitted data. This result impacts very deeply the deployment of WMSN and contributes in a significant increase on the whole network lifetime.

B. Visual Degradation

The second metric that we measured for our approach is, its ability to degrade the ciphered image from the original. In fact, Visual Degradation (VD) measures the visual distortion of the cipher image with respect to the plain image. In other words, even when a passive attacker can capture the transmitted data (i.e., color vector) and even if he knows the encryption technique (i.e., the use of Voronoi tessellation[1]), he could not reconstruct the image because he lacks sites positions. For instance, Figure 9 shows what a passive attacker could see without knowing the positions of the sites with different N values.



(a) Original (b) N=0.25% (c) N=0.5%

(d) N=1% (e) N=1.5% (f) N=2%

Fig. 9: Visual Degradation according to the number of sites.

Similarly, to measure the VD of our approach, and to show the level of similarities between the two images, we have used SSIM metric. We run 1000 times the same Voronoi tessellation by taking the same input color vector. The sites positions were taken randomly. The corresponding SSIM value is then the mean value of these 1000 runs. Figure 10 shows the obtained results.

From the results, we can see that the SSIM index does not exceed 0.2%, even for higher value of N. This result indicates clearly that, using our encryption scheme with any N value, a sufficient and hard visual degradation is attained.

C. Key Sensitivity for the Dynamic Approach

Sensitivity refers to a huge change in the cipher image in response to a slight change on the keys K or IV. The sensitivity of K and IV are analyzed for 1000 random keys and IVs using the Mean Similarity Structural index MSSIM criteria, which represents the mean of the SSIM metric tested before, and the percent Hamming distance that is used to show the number of positions at which the corresponding pixels

[1]Which is far to be easy to know.

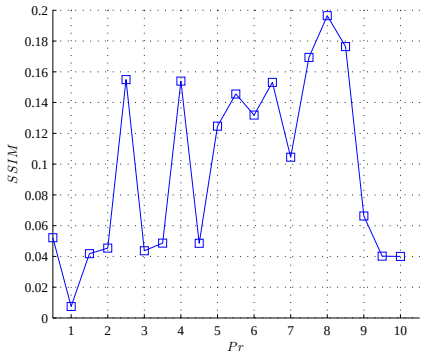


Fig. 10: SSIM index variation according to the number of Voronoi sites (%) in random reconstruction.

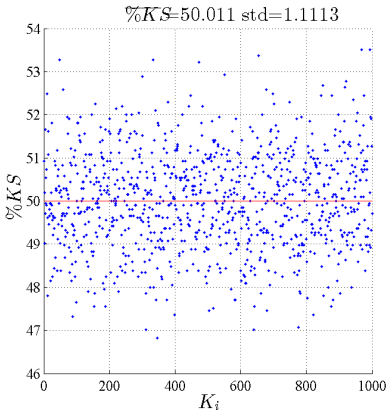


Fig. 11: Key sensibility over 1000 random keys with $N = 1\%$

between the plaintext and ciphertext images are different, and calculated as follows:

$$KS_w = \frac{\sum_{k=1}^{Tb} C_w \oplus C'_w}{Tb} \times 100\% \quad (1)$$

$$= \frac{\sum_{k=1}^{Tb} E_{DK_w\,,\,IV}(P) \oplus E_{DK'_w\,,\,IV}(P)}{Tb} \times 100\%$$

where C_w, C'_w are the corresponding cipher images using dynamic key DK_w and DK'_w respectively. All the elements of DK'_w are equal to those of DK_w, except one element, which is the random Least Significant Bit (LSB). Indeed, the same processing is realized for measuring the sensitivity of IV, giving the same result, since K and IV are mixed together to form the input of the key derivation function.

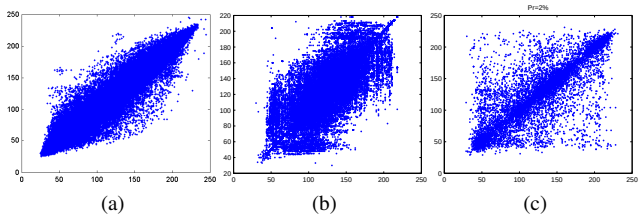
In Figure 11, the sensitivity of the dynamic key versus 1000 random keys is shown, where only the LSB is changed in the used dynamic key DK_i. It can be seen that the majority of samples are close to the optimal value in bit level ($KS_w = 50\%$), and it behaves as a normal distribution with standard deviation $std = 1.1113$.
Similar results are obtained in the case of measuring the plaintext sensitivity, where two similar images that differ only in one bit are chosen. Therefore, the proposed scheme is secure enough, and a chosen/known plain-text attacks has no influence using our approach.

VI. Statistical Properties

In this section, we analyze the intrinsic security characteristics of our dynamic approach in order to demonstrate its safety use. We mainly focus on: (a) random recurrence, (b) distribution, (c) low coefficient correlation between original and encrypted data packets, and (d) errors propagation. In our experiments, the proposed cipher scheme was considered as a black box, where a set of random dynamic keys were chosen randomly.

A. Recurrence

The recurrence plot measures the level of randomness of the cipher, through estimating the correlations between the sequence of data [23]. Considering a packet sequence $x_i = x_{i,1}, x_{i,2}, \ldots, x_{i,m}$, a vector with delay $t \geq 1$ can be constructed as $x_i(t) = x_{i,t},\ x_{i+t+1},\ x_{i,\,t+2}, \ldots,\ x_{i,\,t+m}$. In Figure 12 a-c, the variation between $x_i(t)$ and $x_i(t+1)$ for the original image, the encrypted one and the packets corresponding to N sites are shown. It is obvious that the process of encryption reduces the pattern.



(a) (b) (c)

Fig. 12: (a) Recurrence plot of the original image,(b) its correspondent constructed one and (c) for a packet corresponding to N points with $N = 2\%$

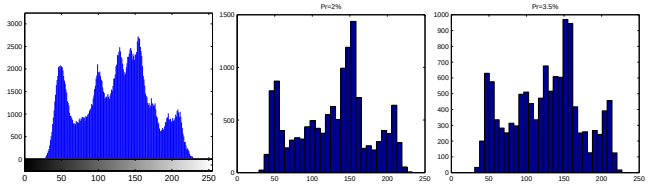
B. Distribution

The mixing nature measures the level of uniformity of the cipher behavior, and it can be quantified by a statistical approach. In Figure 13 a-c, the distribution of the original image and its corresponding cipher image for $N = \%2$ and 3.5% are shown. This result shows clearly that the contents of the encrypted image for both cases are spread over the same space of the original one and have the same distribution.

This means that the frequency counts of the encrypted image (corresponding to N sites) are close to the original distribution. While N increases, it approaches closely from the original one.

C. Low Coefficient Correlation

Another important requirement for any encryption scheme is that, the encrypted data should be greatly different from its original form. The encrypted image must have lower redundancy and a negligible correlation among its adjacent



(a) (b) (c)

Fig. 13: The distribution of the whole original contents image (a) and its correspondent constructed (same of encrypting) one for $N = 1\%$ (b) and $N = 2\%$

pixels. First, the correlation coefficient between the original and the encrypted packets is measured as follows:

$$\rho_{x,y} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \quad (2)$$
$$where\ cov(x,y) = E[\{x - E(x)\}\{y - E(y)\}];$$
$$E(x) = \frac{1}{n} \times \sum_{k=1}^{n} x_i$$
$$and\ D(x) = \frac{1}{n} \times \sum_{k=1}^{n} \{x_i - E[x]\}$$

In Figure 14, the correlation coefficient between the original and encrypted image versus 1000 different keys for Lenna image is shown. It highlights that the correlation coefficient is always close to zero, which indicates that no detectable correlation exists between the original and its corresponding cipher image.

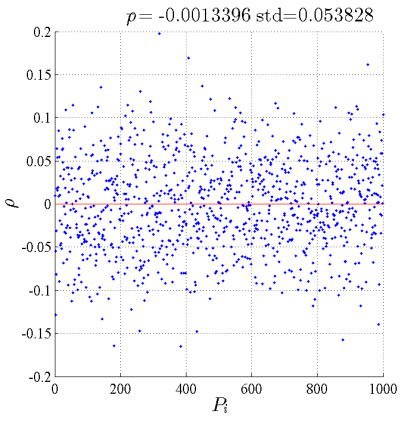


Fig. 14: The coefficient correlation between the original and the encrypted contents image versus 1000 random dynamic keys.

D. Errors Propagation

Additionally, another important criterion, that is not always discussed in the literature but has a direct impact on the transmission, is the error propagation. This criterion stands for the ability of the cipher to support a low propagation of errors in order to be considered as a strong cipher.

Error occurs due to the interference and noise in the transmission channel, which is appeared frequently within WMSNs platforms. A bit error is represented by a simple substitution of a "0" bit by a "1" bit, or *vice versa*. In our proposal, the bit error(s) in the reconstructed sites occur in the same bit position(s) of that of the emitter site, as well as this error remains only on the affected site and does not propagate to other sites. All the remaining sites are not affected. Consequently, our approach is resilient to error propagation risk.

VII. Cryptographic Strength

In this section, we consider typical cryptanalysis cases, previously discussed in the literature [24], [25], and we provide a brief analysis about the proposed scheme against several cryptanalytical attacks.

The proposed scheme is public and an attacker has a complete knowledge about all used techniques, except he don't have any information about the master secret key, in other words, about the sequence of dynamic keys. The use of dynamic-key scheme overcomes the weak points of the static key approach such as accidental key disclosure, and single image failure.

Thus, is well demonstrated in our approach, by using a key derivation function to produce a dynamic key for each tested image (counter mode), which means that different Voronoi diagrams are constructed in a dynamic and random manner, and using different nonlinear dependent master keys. The dynamic key is changed for every tested image, and it is only produced by the source node and regenerated by the sink after an exchange of a secret master key between them. By doing so, this approach could effectively prevents the problem of single image failure.

Moreover, the proposed cipher ensures several statistical characteristics compared to the original image such as uniformity and random recurrence. Thus, leading to achieve a good immunity against statistical attacks. Furthermore, differential and linear attacks become ineffective, and the breaking of the system appears to be a very hard task, comparing to existing solutions, due to the key sensibility, and the use of the counter mode, that produces a different set of sites for each input image. In fact, any change in any bit of the dynamic key or IV (public parameters) causes a significant difference in the set of sites and consequently in the encrypted image as seen in Figure 11.

Besides, the use of a dynamic cipher structure limits the ability of the attackers to break out the cipher. Hence, security is achieved with one simple process instead of using AES scheme, with many iterations. Thus, leads to a very low complexity scheme whilst ensuring a high level of security.

Finally, a large master secret key and a large dynamic key are used in our proposition, where the key space of the master secret key can be 2^{128}, 2^{256} or 2^{512}. So, it is sufficiently large to make the brute-force attack unfeasible. Additionally, the key

space of the dynamic key is 2^{512}, which can also be considered as large enough to resist against brute-force attack.

Noting that, the difficulty of cipher-text-only attack is equal to one of the brute force attacks. Hence, it becomes impossible for a cipher-text-only attack to extract any useful information. Therefore, the cipher scheme has the strength against several types of powerful attacks.

VIII. Conclusion and Future Works

In this paper, a low computational image encryption cipher algorithm was presented, and discussed. This proposed scheme ensures the security with lower computational complexity and without the use of any traditional compression techniques and security standards.

Moreover, this proposed scheme is composed of two components: a dynamic key derivation function, and a dynamic Voronoi Diagram. A new method, based on a simple algebraic rule, to construct a dynamic Voronoi diagram is presented. Also, the stream cipher RC4 layer is used to produce a set of points (x, y) that are used to build the Voronoi tessellation.

This algorithm provides a good level of security with a little communication overhead (only the color vector is transmitted). In addition, the dynamic key sensitivity is attained since the produced Voronoi diagram depends on the dynamic key, which varies for each input image.
Simulation results evaluates the effectiveness of the proposed cipher scheme and its robustness against different types of attacks such as statistical, chosen/known plain-text attack, brute-force attack, and cipher-text-only attack.

Moreover, the proposed cipher algorithm has a low computational complexity and consequently requires more energy saving compared to the existing solutions that are based on AES scheme, or compression standards, which require more complexity and more energy consumption. Also, Our proposition is considered as an adequate candidate for modern privacy multimedia scheme that is implemented to ensure secure data transmission in WMSNs.

In future, our work will be extended to design an authentication-privacy scheme to ensure a better reduction in the computational complexity, as well as enhancing the remaining two aspects of security: data integrity and source authentication.

References

[1] M. Guerrero-Zapata, R. Zilan, J. M. Barceló-Ordinas, K. Bicakci, and B. Tavli, "The future of security in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 45, no. 1, pp. 77–91, 2010.

[2] G. K. Wallace, "The jpeg still picture compression standard," *Communications of the ACM*, vol. 34, no. 4, pp. 30–44, 1991.

[3] D.-U. Lee, H. Kim, D. E. Mohammad Rahimi, and J. D. Villasenor, "Energy-efficient image compression for resource-constrained platforms," *IEEE TRANSACTIONS ON IMAGE PROCESSING*, vol. 18, no. 9, 2009.

[4] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *Image Processing, IEEE Transactions on*, vol. 13, no. 4, pp. 600–612, 2004.

[5] 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.

[6] R. Di Pietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure wireless sensor networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. ACM, 2003, pp. 62–71.

[7] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2004, pp. 43–52.

[8] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 41–77, 2005.

[9] S. Zhu, S. Setia, and S. Jajodia, "Leap+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[10] H. Chan and A. Perrig, "Pike: Peer intermediaries for key establishment in sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 1. IEEE, 2005, pp. 524–535.

[11] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. ACM, 2003, pp. 141–150.

[12] G. Gaubatz, J.-P. Kaps, and B. Sunar, "Public key cryptography in sensor networksrevisited," in *Security in Ad-hoc and Sensor Networks*. Springer, 2005, pp. 2–18.

[13] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2004, pp. 59–64.

[14] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*. IEEE, 2004, pp. 71–80.

[15] D. Kundur, W. Luh, U. N. Okorafor, and T. Zourntos, "Security and privacy for distributed multimedia sensor networks," *Proceedings of the IEEE*, vol. 96, no. 1, pp. 112–130, 2008.

[16] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang, "Framework for security and privacy in automotive telematics," in *Proceedings of the 2nd international workshop on Mobile commerce*. ACM, 2002, pp. 25–32.

[17] D. A. Fidaleo, H.-A. Nguyen, and M. Trivedi, "The networked sensor tapestry (nest): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks," in *Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks*. ACM, 2004, pp. 46–53.

[18] Q. Du, M. Gunzburger, L. Ju, and X. Wang, "Centroidal voronoi tessellation algorithms for image compression, segmentation, and multichannel restoration," *Journal of Mathematical Imaging and Vision*, vol. 24, no. 2, pp. 177–194, 2006.

[19] H. Gilbert and H. Handschuh, "Security analysis of sha-256 and sisters," in *Selected areas in cryptography*. Springer, 2004, pp. 175–193.

[20] S. S. Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, and B. P. Sinha, "High-performance hardware implementation for rc4 stream cipher," *IEEE Transactions on Computers*, vol. 62, no. 4, pp. 730–743, 2013.

[21] S. S. Hemami and A. R. Reibman, "No-reference image and video quality estimation: Applications and human-motivated design," *Signal processing: Image communication*, vol. 25, no. 7, pp. 469–481, 2010.

[22] S. Chikkerur, V. Sundaram, M. Reisslein, and L. J. Karam, "Objective video quality assessment methods: A classification, review, and performance comparison," *Broadcasting, IEEE Transactions on*, vol. 57, no. 2, pp. 165–182, 2011.

[23] A. Hyvärinen, J. Hurri, and J. Väyrynen, "Bubbles: a unifying framework for low-level statistical properties of natural image sequences," *JOSA A*, vol. 20, no. 7, pp. 1237–1252, 2003.

[24] X. Wang and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 24, pp. 5804–5807, 2011.

[25] A. Bogdanov and M. Wang, "Zero correlation linear cryptanalysis with reduced data complexity," in *Fast Software Encryption*. Springer, 2012, pp. 29–48.