SECURE IMAGE TRANSMISSION SCHEME IN UNMANNED AERIAL VEHICLES USING MULTIPLE SHARE CREATION WITH OPTIMAL ELLIPTIC CURVE CRYPTOGRAPHY

M. S. Minu

Research Scholar of Computer Science and Engineering, Sathyabama Institute of Science and Technology,
Chennai, India
msminu1990@gmail.com

R. Aroul Canessane

Professor of Computer Science and Engineering, Sathyabama Institute of Science and Technology,
Chennai, India
aroulcanessane@gmail.com

Abstract

Unmanned aerial vehicles (UAVs) normally fly at low altitudes to acquire high-resolution images covering small regions. The applicability of commercial UAVs finds useful in different domains such as asset management, construction management, real estate, property assessment, as well as disaster response. Security is a major issue exist in the design of UAV networks and can be resolved by the use of effective image encryption technique. In this view, this paper focuses on the design of multiple share creation (SC) scheme with social spider optimization (SSO) based optimal elliptic curve cryptography (ECC) technique, called SC-SSOECC for secure image transmission scheme in UAVs. The SC-SSOECC technique initially separates the color bands (R, G, and B) for every image. Then, the generation of multiple shares takes place for every image which turns to be complex for the hackers to retrieve the original image. In addition, the secrecy of the images can be increased by the use of ECC technique where the optimal key generation process in ECC takes place using SSO algorithm. The SC-SSOECC algorithm is found to be highly secure and useful for practical image encryption in real time systems. An extensive experimental analysis stated the proficient performance of the SC-SSOECC model and the results are examined interms of mean square error (MSE), peak signal to noise ratio (PSNR), and correlation coefficient (CC).

***Keywords*: Unmanned Aerial Vehicles, Security, Image encryption, Share creation, Key generation.**

1. Introduction

Unmanned Aerial Vehicles (UAV) are also named as drones, which are applied for armed forces like mapping, surveillance, search and rescue as well as target observation. In recent times, drones are employed in civilian applications. In 2016, Facebook's solar-powered unmanned plane Aquila made the basic test flight an alternative Internet delivery environment for most of the remote portions of the world. Followed by, communication payload applied by Aquila employs lasers for sending data robustly when compared with previous models [Zuckerberg (2016)]. In addition, Qualcomm techniques are meant to be a subsidiary of Qualcomm Incorporated and AT&T, published that it may be a test of Unmanned Aircraft Systems (UAS), on commercial 4G LTE system [Vanian (2016)]. UAV system is applied in major applications like disaster management [Asadpour *et al.* (2013); Erdelj *et al.* (2017)], common services, farming, and infrastructure damage estimation [Lim *et al.* (2016); Kong *et al.* (2002)]. By comparing the infrastructure based overlay system, UAVs are employed to develop wireless system to make use of network topology effectively and allocate wireless parameters in dynamic fashion. Next, application of UAV is to create temporary system which is cheaper and demands low time when compared with symmetric wired structure of remote area.

[Gupta *et al.* (2015)] established a sequence of communication and network demands for UAV systems. The above demands are features like dynamic networking, supremacy of wireless communications, flight management, and so on. [Rosati *et al.* (2015)] deployed the expansion of Optimized Link-State Routing Protocol (OLSR) which has computed routing effectively even under dynamic conditions. Actually, the newly deployed protocol determines the routing by weighing the Expected Transmission Count (ETX). In 2016, unlike from distributed routing protocol, [Lee *et al.* (2016)] used a centralized routing protocol by applying ground control mechanism to develop effective network. [Xu and Carrillo (2017)] proposed online finite horizon best flocking control as well as remarkable co-design for effective UAV system. The UAV networks are well-known model which is employed in most of the applications where the security issues are also enhanced. With no security mechanisms, an intruder simply hacks the users' confidential data. [Rodday (2016)] computed a live attack by applying professional drone's susceptibilities to the UAV networks. The actual consequences of these intrusions are highly terrible. Terrorist groups have captured the unencrypted UAV video and transferred it from a US drone to US military satellite with the help of SkyGrabber [Arthur (2009)]. The basic security model for UAV system concentrates on security, trust, confidentiality of data using cryptography. A well-developed data protection approach ensures that an intruder can never access the data unless using a reputed hacking approach.

[Won *et al.* (2015)] deployed an effective Certificate-less Signcryption Tag Key Encapsulation model which is a protective communication protocol for drones as well as modern objects. Therefore, the protocol is yet unable to send huge amounts of encrypted data to receivers at the time of preserving security of end devices. Followed by, many other new cryptographic key management approaches. For allocating symmetric encryption keys for group of classes, [Castiglione *et al.* (2015)] projected new hierarchical key assignment mechanism with the help of symmetric encryption method as well as perfect secret sharing approach. Here, a system master produces a symmetric key for collective entities and met the requirement of complex structure. [Castiglione *et al.* (2016)] create a hierarchical key assignment method in conjunction with dynamic updates, where the user demands storing single private key. Therefore, above 2 methods are named as symmetric encryption approaches and it limits the burden of symmetric key management. [Wu *et al.* (2009)] presented novel cryptographic asymmetric primitive implied as asymmetric group key agreement. According to the novel primitive, [Wu *et al.* (2012)] established a new asymmetric group key agreement framework to resolve the barriers of potentially limited communication from sender with inexistence of a trusted third party and support the dynamic key update. But, group infrastructure is a circuit which supports the hierarchical group infrastructure.

This paper aims to develop an effective multiple share creation (SC) with social spider optimization (SSO) based elliptic curve cryptography (ECC) technique, called SC-SSOECC for secure image transmission scheme in UAVs. The presented model performs three major processes such as band separation, share creation, and encryption. The SC-SSOECC technique firstly partitions the color bands (R, G, and B) for every image. Then, the generation of multiple shares takes place for every image to achieve security. Moreover, optimal ECC with SSO based key generation process is involved to encrypt the generated shares, and thereby the secrecy can be further improved. In order to ensure the supremacy of the SC-SSOECC model, a series of simulations were performed on the benchmark aerial image dataset.

2. The Proposed SC-SSOECC model

Fig. 1 depicts the workflow of the presented SC-SSOECC model. Primarily, the input secret image is developed and collection of 12 shares are produced with few individual shares of color band. Followed by, multiple shares have been generated to accomplish protective image transmission and image shares are divided as groups of blocks. Followed by, the blocks of a share are subjected to encryption and decryption process with the help of SSOECC approach. When the share is encrypted, then it is forwarded to the destination, and reconstruction is computed for acquiring the actual input image. When the decryption is completed, the secret shares would be retrieved. Next, shares of secret images have been stacked jointly to redevelop the input image significantly.

2.1. *Share Generation*

Basically, the pixel value of actual images is filtered and produce the RGB values in a matrix form. Hence, the matrix size and input image are considered to be symmetric. Followed by, the input pixel value of an image is described by,

$$Pixel = \sum R + G + B \tag{1}$$

The pixels available in input image are displayed in n different manners named as shares. Each share is composed of a collective sub-pixel of RGB images. Hence, the RGB shares have relied on pixel values in RGB images. Additionally, the RGB shares are described by R_s, $G_{s,}$ and B_s as given below.

$$R_s = \int_1^k lim_{k\to 1ton} R_{ab} \tag{2}$$

$$G_s = \int_1^k lim_{k\to 1ton} G_{ab} \tag{3}$$

$$B_s = \int_1^k lim_{k\to 1ton} B_{ab} \tag{4}$$

where a and b refers the position of matrix, $R_s, G_s\ and\ B_s$ defines the shares of RGB, $R_{ab}, G_{ab}\ and\ B_{ab}$ are said to be elements of an image pixel [Shankar and Eswaran (2017)]. ECC method has been for computing share encryption. In general, a share does not exhibit useful information till all the generated shares are combined. Before developing the shares, fundamental matrix is illustrated by means of share count. Additionally, a random key has been allocated based on the block size of an input image. Therefore, number of shares can be implied by 2^s, when the $S \geq 2$. The general matrix form can be achieved when RGB values from pixels are portioned by S. Then, shares are produced by computing XOR operation of matrix on diverse integration. In this approach, fundamental matrix count is illustrated as 2 and share value is 4. The matrix form has been generated by classifying RGB values of pixel by 2. In prior to computing share creation, the upcoming process has been carried out on the XR_1 and XR_2 matrices. The red band shares have been produced by computing XOR process with fundamental and key matrices. The above-mentioned process gets repeated for both green as well as blue bands of the input images.

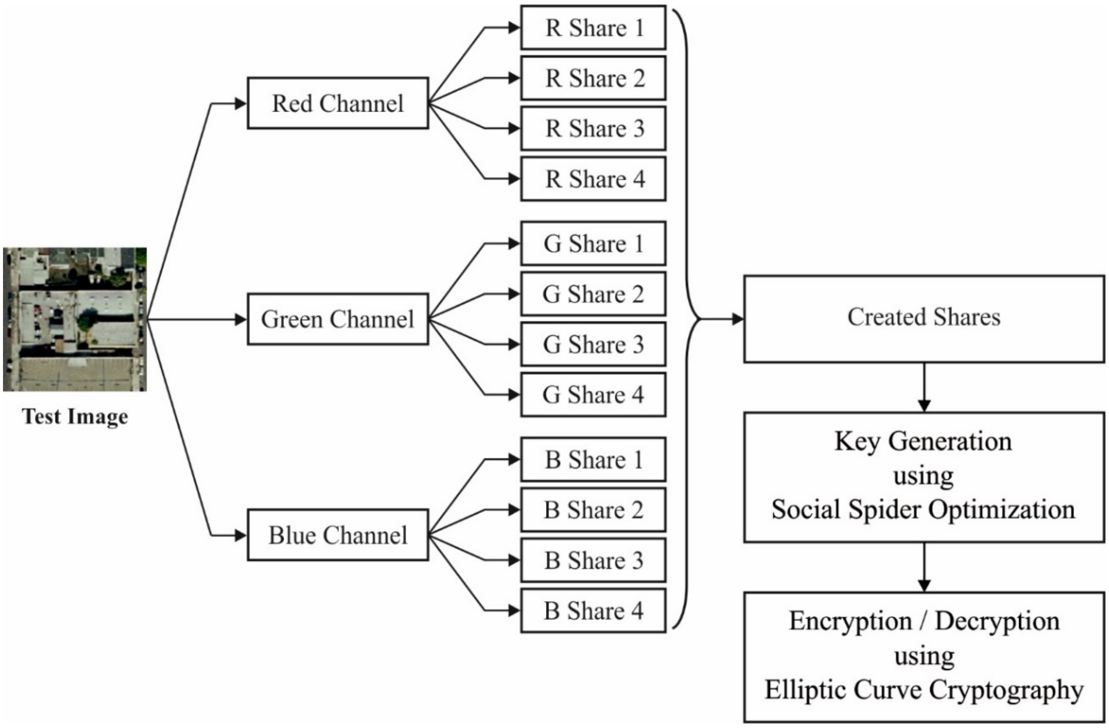

Fig. 1. Overall Process of Proposed SC-SSOECC model.

2.2. *Share Reconstruction*

In case of reconstruction, several shares are piled up for generating the actual image. When the shares are produced for an input image, ECC method has been employed for encryption as well as decryption of shares.

2.3. *Encryption/Decryption*

The elliptic curve method (ECM) is connected to cryptography called ECC which has been applied for implementing the public key cryptography. Here, security is emulated from EC mechanism and referred as Discrete Logarithm Problem (DLP) in simplified EC. As a result, the periodical limitation in key size can be reached with similarity level of security offered in public key cryptography. Hence, a curve is depicted by the function as given in the following:

$$Y^2 modp = X^3 + aX + bmodp, \tag{5}$$

where a, b defines the integers and p means the prime value. In ECC, a prime value has been selected as k and private key is selected as L. Then, ECC function is demonstrated by

$$F = (S(i))^3 + u * S(i) + v, \tag{6}$$

where u and v stand for constants offered by $u = v = 2.$ One of the major benefits of ECC is that it is comprised of small key size, compact memory space as well as transmission requirements. If $X = Y$ is satisfied, then best point is selected for EC. Additionally, X and $Y$are illustrated as,

$$X = mod(F, n_p), \tag{7}$$

$$Y = mod\ ((S(j))^2, n_p), \tag{8}$$

where $p(i,j)$refers the point of EC and n_p signifies the prime value. Therefore, doubling process is employed to find the values of X and Y.

2.4. *SSO based Key generation process*

In order to encrypt and decrypt the shares, private key has been developed and applied by using prime value from the image. In case of encryption, arbitrary generation of public key is performed and decryption processes apply SSO for private key generation of ECC method. To enhance the efficiency of ECC model, the SSO is applied as a private key (H) generator. The best private key generation task depends upon the 'fitness function (FF)' as optimal key with peak signal to noise ratio (PSNR) and utilized to scramble and unscramble the data. Hence, SSO approach is applied for selecting the keys and FF is depicted in the following.

$$Fitness = MAX\{PSNR\} \tag{9}$$

Generally, SSO is defined as a metaheuristic approach which initializes the nature of social spider to reside jointly, explore the food, and send the required data. Actually, the population of social spiders is classified into 2 classes namely, female and male, in which females are higher than male population. These groups develop a web (search domain) and explore the food on the web. Hence, the solutions of SSO can be referred by the location of a spider in web, which sends the data regarding prey and location of a spider to adjacent spiders [Luque-Chang *et al.* (2018)].

3. Experimental Validation

For examining the performance of the SC-SSOECC model, a set of simulations were performed on benchmark UAV dataset [http://weegee.vision.ucmerced.edu/datasets/landuse.html]. In addition, the experimental results are validated interms of different metrics such as mean square error (MSE), PSNR, and correlation coefficient (CC). The value of MSE should be low, and the values of PSNR/CC should be high for better performance.

Table 1 visualizes the share creation process of the SC-SSOECC model on the applied sample image. The tables denote the generation of the different shares for the applied input image. For each image, a set of 12 shares, (i.e. four shares under R, G, and B) are generated.

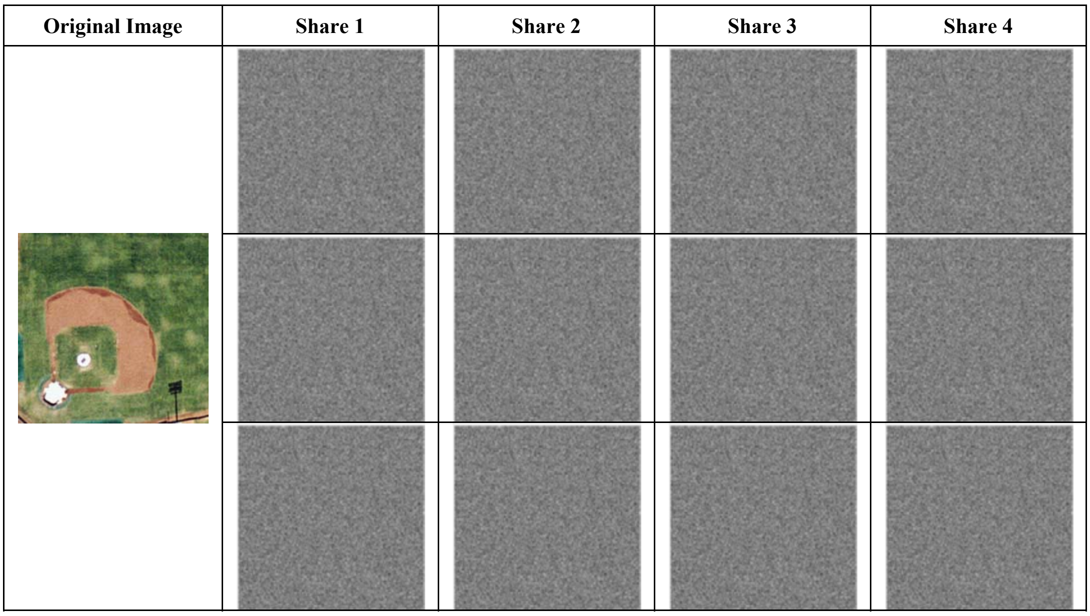

Table 1. Visualization of Share Creation Scheme on Sample Image-1.

Row 1 represents the shares created for R band, row 2 denotes the shares generated for G band, and finally, B represents the shares produced for B band. After observing the shares exist in the table, it is apparent that the shares depict zero meaning and none of the information can be attained by the shares.

Table 2 depicts the analysis of the results by the SC-SSOECC model interms of MSE, PSNR, and CC. The presented SC-SSOECC model has achieved minimum MSE with maximum PSNR and CC. For the test sample image 1, the SC-SSOECC model exhibits a better outcome by obtaining an MSE of 0.087, PSNR of 58.736dB, and CC of 0.993. Eventually, the test sample image 2, the SC-SSOECC model shows moderate outcome by obtaining an MSE of 0.123, PSNR of 57.232dB, and CC of 0.996. Along with that, the test sample image 3, the SC-SSOECC model displays a considerable outcome by gaining an MSE of 0.094, PSNR of 58.400dB, and CC of 0.994. Followed by, the test sample image 4, the SC-SSOECC method showcased the acceptable result by obtaining an MSE of 0.183, PSNR of 55.506dB, and CC of 0.996. Simultaneously, in the test sample image 5, the SC-SSOECC method exhibits a better outcome by accomplishing an MSE of 0.163, PSNR of 56.009dB, and CC of 0.997.

Test Images	MSE	PSNR	CC
Image 1	0.087	58.736	0.993
Image 2	0.123	57.232	0.996
Image 3	0.094	58.400	0.994
Image 4	0.183	55.506	0.996
Image 5	0.163	56.009	0.997

Table 2. Result Analysis of Proposed Method SC-SSOECC.

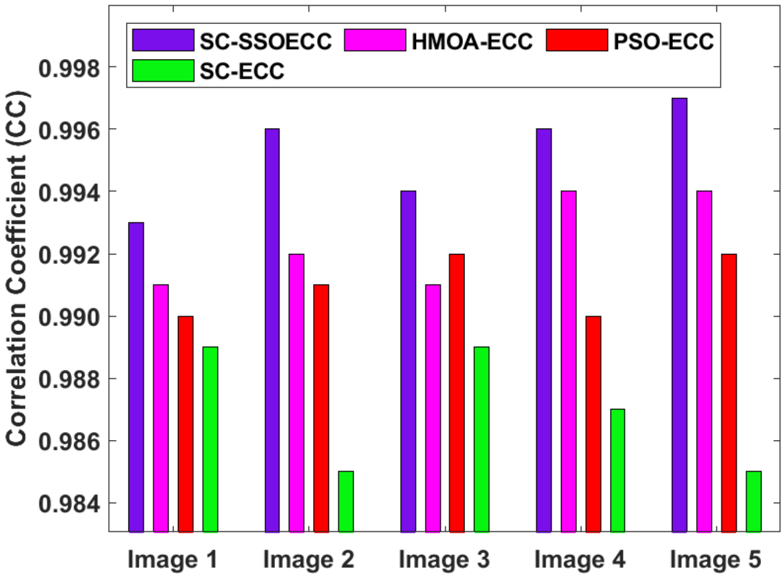

Fig. 2. Result analysis of SC-SSOECC model interms of CC.

Fig. 2 examine the outcome of the SC-SSOECC method with existing model by means of CC. The final outcome has implied that the SC-ECC model has appeared as the worst performer over the other methods. Meantime, the PSO-ECC model has managed to showcase slightly enhanced outcomes over the SC-ECC model. Simultaneously, the HMOA-ECC model has reached a competing performance over the existing methods. Lastly, the presented SC-SSOECC model has accomplished effective results by offering maximum CC. For instance, on the applied image 1, a higher CC of 0.993 is accomplished by the SC-SSOECC model whereas the HMOA-ECC, PSO-ECC, and SC-ECC models have led to a minimum CC of 0.991, 0.990, and 0.989 respectively. Finally, on the applied image 5, a higher CC of 0.997 is achieved in the SC-SSOECC model whereas the HMOA-ECC, PSO-ECC, and SC-ECC models have led to a low CC of 0.994, 0.992, and 0.985 respectively.

4. Conclusion

This paper has presented a new SC-SSOECC technique for secure image transmission scheme in UAVs. The presented model performs three major processes such as band separation, share creation, and encryption. Initially, the bands are separated in the RGB images and then shares are created for every band. Followed by, ECC technique is utilized to encrypt the generated shares. In order to improve the performance of the ECC, an optimal key generation process takes place by the SSO algorithm. The SC-SSOECC algorithm is found to be highly secure and useful for practical image encryption in real-time systems. For examining the performance of the SC-SSOECC model, a set of simulations were performed on benchmark UAV dataset. In addition, the experimental results are validated interms of different metrics such as MSE, PSNR, and CC. The experimental results ensured that the SC-SSOECC model is found to be secure over the compared methods. As a part of future work, image classification models can be developed to determine the class labels of the aerial images.

References

[1] Arthur, C. (2009): SkyGrabber: the $26 software used by insurgents to hack into US drones. The Guardian, 17.

[2] Asadpour, M.; Giustiniano, D.; Hummel, K. A.; Egli, S. (2013): UAV networks in rescue missions. In Proceedings of the 8th ACM international workshop on Wireless network testbeds, experimental evaluation & characterization (pp. 91-92).

[3] Castiglione, A.; De Santis, A.; Masucci, B.; Palmieri, F.; Castiglione, A.; Li, J.; Huang, X. (2015): Hierarchical and shared access control. IEEE Transactions on Information Forensics and Security, **11**(4), pp.850-865.

[4] Castiglione, A.; De Santis, A.; Masucci, B.; Palmieri, F.; Castiglione, A.; Huang, X. (2016): Cryptographic hierarchical access control for dynamic structures. IEEE Transactions on Information Forensics and Security, **11**(10), pp.2349-2364.

[5] Erdelj, M.; Natalizio, E.; Chowdhury, K. R.; Akyildiz, I. F. (2017): Help from the sky: Leveraging UAVs for disaster management. IEEE Pervasive Computing, **16**(1), pp.24-32.

[6] Gupta, L.; Jain, R.; Vaszkun, G. (2015): Survey of important issues in UAV communication networks. IEEE Communications Surveys & Tutorials, **18**(2), pp.1123-1152.

[7] http://weegee.vision.ucmerced.edu/datasets/landuse.html

[8] Kong, J.; Luo, H.; Xu, K.; Gu, D. L.; Gerla, M.; Lu, S. (2002): Adaptive security for multilevel ad hoc networks. Wireless Communications and Mobile Computing, **2**(5), pp.533-547.

[9] Lee, J.; Kim, K.; Yoo, S.; Chung, A. Y.; Lee, J. Y.; Park, S. J.; Kim, H. (2016): Constructing a reliable and fast recoverable network for drones. In 2016 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[10] Lim, G. J.; Kim, S.; Cho, J.; Gong, Y.; Khodaei, A. (2016): Multi-UAV pre-positioning and routing for power network damage assessment. IEEE Transactions on Smart Grid, **9**(4), pp.3643-3651.

[11] Luque-Chang, A.; Cuevas, E.; Fausto, F.; Zaldivar, D.; Pérez, M. (2018): Social spider optimization algorithm: modifications, applications, and perspectives. Mathematical Problems in Engineering, 2018.

[12] Rodday, N. (2016): Hacking a professional drone. Black Hat Asia, 2016.

[13] Rosati, S.; Krużelecki, K.; Heitz, G.; Floreano, D.; Rimoldi, B. (2015): Dynamic routing for flying ad hoc networks. IEEE Transactions on Vehicular Technology, **65**(3), pp.1690-1700.

[14] Shankar, K.; Eswaran, P. (2017): RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, **14**(2), pp.118-130.

[15] Vanian, J. (2016): Qualcomm and AT&T are joining forces on a new drone project. http://fortune.com/2016/09/06/qualcomm-att-drone-tests/

[16] Won, J.; Seo, S. H.; Bertino, E. (2015): A secure communication protocol for drones and smart objects. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 249-260).

[17] Wu, Q.; Mu, Y.; Susilo, W.; Qin, B.; Domingo-Ferrer, J. (2009): Asymmetric group key agreement. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 153-170). Springer, Berlin, Heidelberg.

[18] Wu, Q.; Qin, B.; Zhang, L.; Domingo-Ferrer, J.; Manjón, J. A. (2012): Fast transmission to remote cooperative groups: a new key management paradigm. IEEE/ACM Transactions on networking, **21**(2), pp.621-633.

[19] Xu, H.; Carrillo, L. R. G. (2017): Fast reinforcement learning based distributed optimal flocking control and network co-design for uncertain networked multi-UAV system. In Unmanned Systems Technology XIX (Vol. **10195**, p. 1019511). International Society for Optics and Photonics.

[20] Zuckerberg, M. (2016): The technology behind Aquila.