|  |  |
| --- | --- |
| **Group** 8 | **Death Star Image Exfiltration** |
| **Major:** | **Team members:** |
| EE | Nicholas Michael |
| CEG | Mason McDaniel |
| IT/Cyber | Chase Ennis |
| IT/Cyber  CS | Cade Wrinkle  Michael Mowad |

**System Design Trades**

**Wireless Transmission**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Solution**  **[Requirement]** | **Rated Data Throughput**  **[90]** | **Cost** | **Native Encryption Support [80]** | **Existing Software Libraries / SDKs [Opt]** | **Existing Tutorials [Opt]** | **Follows WSU environment and safety regulations** |
| Enhanced Shockburst (ESB) | 2 Mbps and 1 Mbps [2] | $46.37 [3] | Yes [2] | Yes [1] | Yes [1] | Yes |
| Zigbee | 250 Kbps [4] | $100 for kit [4] | AES-128/256 [4] | Yes [4] | Yes [5] | Yes |
| Software Defined Radio | Up to 400 Gb/s [6] | $159.99 [8] | No [7] | Yes [7] | Yes [7] | Yes |
| QR Code | 180 Kbps \* [10] | $12.49 [10] | No [9] | Yes [9] | Yes [9] | Yes |
| Laser IRDA | 9600 bps – 16 Mbps [11] | 80€ [12] | No [11] | No | Yes [13] | No |

\* The data throughput of the QR code was calculated using the size of the QR code (3 kbs) and the speed of the raspberry pi camera (60 fps) allowing for a max data throughput of 180 kbps.

Wireless Transmission Design Explanation:

To transmit at least 10 1024x1024 images over a 600 second interval, the datarate of the transmission should be in excess of 420 Kbps. QR codes were removed from consideration due to the low supported data rate. IrDA can operate with a wide range of data rates, some of which are satisfactory and others that are unsatisfactory; it is implementation dependent. IrDA would require more effort for to implement the communication protocol atop the hardware layer than ESB and Zigbee, due to the lack of satisfactory libraries. For a single channel, the data rate of Zigbee is below the minimum viable rate. Additionally, the barrier cost of Zigbee is higher than ESB, so ESB is preferred over Zigbee.

Wireless Transmission Sources:

[1] “Enhanced Shockburst.” Nordic semiconductor. [Online]. Available: <https://docs.nordicsemi.com/bundle/ncs-latest/page/nrf/protocols/esb/index.html>. Accessed: October 14, 2024.

[2] “nRF52840 Product Specification.” Nordic semiconductor. [Online]. Available: <https://docs.nordicsemi.com/bundle/ps_nrf52840/page/keyfeatures_html5.html> Accessed: October 14, 2024.

[3] “Nordic Semiconductor nRF52840-DK.” Mouser Electronics. [Online]. Available: <https://www.mouser.com/ProductDetail/Nordic-Semiconductor/nRF52840-DK?qs=F5EMLAvA7IA76ZLjlwrwMw%3D%3D&utm_source=OEMSecrets&utm_medium=aggregator&utm_campaign=nRF52840DK&utm_term=nRF52840DK&utm_content=Nordic%20Semiconductor>. Accessed: October 14, 2024.

[4] *“*DIGI XBEE 3 ZIGBEE MESH KIT.” Digikey. [Online]. Available: <https://mm.digikey.com/Volume0/opasdata/d220001/medias/docus/6346/XK3-Z8S-WZM.pdf>. Accessed: October 14, 2024.

[5] “How to Transform a RaspberryPi Into a Universal Zigbee and Z-Wave Bridge.” Hackernoon. [Online]. Available: <https://hackernoon.com/how-to-transform-a-raspberrypi-into-a-universal-zigbee-and-z-wave-bridge-xy1ay3ymz>. Accessed: October 14, 2024.

[6] “Design Considerations for High-Throughput SDR Systems.” ElectronicDesign. [Online]. Available: <https://www.electronicdesign.com/markets/automation/article/21157953/per-vices-corp-design-considerations-for-high-throughput-sdr-systems> Accessed: October 16, 2024

[7] “Radioberry.” GitHub Repository. [Online]. Available: <https://github.com/pa3gsb/Radioberry-2.x/wiki>. Accessed: October 14, 2024.

[8] “AURSINC SDR Radioberry V2.0 for Raspberry Pi 4/4B, Radio Card (Raspberry Pi 4 Hat) Analog Devices AD9866 & 10CL025 12-bit Broadband Modem for Ham Radio SDR Transceiver Software Defined Radio” Amazon.com. [Online]. Available: <https://www.amazon.com/AURSINC-SDR-Radioberry-Raspberry-Broadband/dp/B0C2PTW8XW?crid=S5NQ5XHCOP2L&keywords=radioberry&qid=1690015516&sprefix=radioberry%2Caps%2C225&sr=8-1-spons&sp_csd=d2lkZ2V0TmFtZT1zcF9hdGY&linkCode=sl1&tag=techminds-20&linkId=618f2541c7623ab87b49017bc46d8e90&language=en_US&ref_=as_li_ss_tl&th=1.> Accessed: Oct. 16, 2024.

[9] Rust, Evan. “Scan QR Codes in Real-Time with Raspberry Pi.” Hackster.io. [Online]. Available: <https://www.hackster.io/gatoninja236/scan-qr-codes-in-real-time-with-raspberry-pi-a5268b>. Accessed: Oct. 16, 2024.

[10] Tripathi, Pankaj. “How Much Data Can QR Code Hold?” UNIQODE. Available: <https://www.uniqode.com/blog/qr-code/how-much-data-can-qr-code-hold>. Accessed: Oct. 16, 2024

[11] Suvak, Dave. “IrDA and Bluetooth: A Complementary Comparison.” Extended Systems. [Online]. Available: <http://alumni.cs.ucr.edu/~csyiazti/courses/cs260/downloads/IrDA_vs_Bluetooth.pdf>. Accessed: Oct. 14, 2024.

[12] “USB IrDA Kit.” IRDroid. [Online]. Available: <https://irdroid.eu/product/usb-irda-kit/>. Accessed: Oct. 16, 2024.

[13] “Unit 5: IrDA Communications Protocols.” Digilent. [Online]. Available: <https://digilent.com/reference/microprocessor/basys-mx3/unit-5/start>. Accessed: Oct 16, 2024.

**Image Recognition**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Option*** | ***Sample Size*** | ***Speed & Efficiency***  ***[Opt]*** | **Ease of Integration**  **[Opt]** | **Training Time** | **Accuracy & Percision** |
| K-Nearest Neighbor | Poor [10] | Slow [10] | Easy [15] | No training required [15] | Moderate [10] |
| Decision Tree | Good [13] | Fast [10] | Easy [13] | Moderate [13] | High [10] |
| Support vector machine | Moderate [11] [12] | Slow (Complex Kernels) [14] | Complex [14] | Long [14] | Very High [11] |
| Random Forest | Large [9] | Slow [9] | Complex [9] | Moderate [5] | High [7] |
| Linear Discriminant Classifier | Moderate [3] | Fast [6] | Easy [6] | Moderate [3] | High [5] |
| Logisitic Regression | Large [2] | Fast [2] | Easy [8] | Fast [8] | Moderate [1] |

The chart compares several Image Recognition methods including “K-Nearest Neighbor (KNN)”, “Decision Tree”, “Support Vector Machine”, “Random Forest”, “Linear Discriminant Classifier”, and “Logistic Regression”. They are rated based on Sample Size, Speed & Efficiency, Ease of Integration, Training Time, and Accuracy & Precision. If an option got a “poor” rating for Sample size, it means that it can only handle a small data set, and vice versa. If an option is “slow” for Speed & Efficiency, that means that the option is a time-consuming option, and vice versa. If an option is “complex” for Ease of Intergration, that means that it may be difficult to intergrade into the project. If an option is “Long” for Training Time, that means that it takes a while to train the dataset. And lastly, Accuracy & Precision is self-explanatory.

[1] A. Satya, J. Prakash, and P. Sriramya, “Accuracy Analysis for Image Classification and Identification of Nutritional Values Using Convolutional Neural Networks in Comparison with Logistic Regression Model,” *Journal of Pharmaceutical Negative Results*, vol. 13, no. SO4, doi: 10.47750/pnr.2022.13.s04.067. Available: <https://www.pnrjournal.com/index.php/home/article/view/951> Accessed: Oct 18, 2024

[2] A. Thanda, “What is Logistic Regression? A Beginner's Guide [2023],” *CareerFoundry*, May 11, 2023. Available: <https://careerfoundry.com/en/blog/data-analytics/what-is-logistic-regression/> Accessed: 10/18/2024

[3] D. Cai, X. He and J. Han, "Training Linear Discriminant Analysis in Linear Time," *2008 IEEE 24th International Conference on Data Engineering*, Cancun, Mexico, 2008, pp. 209-217, doi: 10.1109/ICDE.2008.4497429. Available: <https://ieeexplore.ieee.org/document/4497429> Accessed: Oct 18, 2024

[4] D. Yates and M. Z. Islam, “FastForest: Increasing random forest processing speed while maintaining accuracy,” *Information Sciences*, vol. 557, pp. 130–152, Dec. 2020, doi: 10.1016/j.ins.2020.12.067. Available: <https://www.sciencedirect.com/science/article/pii/S0020025520312330> Accessed: Oct 18, 2024

[5] E. Kavlakoglu, “Implementing linear discriminant analysis (LDA) in Python,” *IBM Developer*, Mar. 18, 2024. Available: <https://developer.ibm.com/tutorials/awb-implementing-linear-discriminant-analysis-python/> Accessed: Oct 18, 2024

[6] “Linear Discriminant analysis in machine learning,” *GeeksforGeeks*, Mar. 20, 2024. Available: <https://www.geeksforgeeks.org/ml-linear-discriminant-analysis/#advanatages-disadvantages-of-using-lda> Accessed: Oct 18, 2024

[7] N. Beheshti, “Random Forest Classification - towards data science,” *Medium*, Jan. 29, 2022. [Online]. Available: <https://towardsdatascience.com/random-forest-classification-678e551462f5> Accessed: Oct 18, 2024

[8] “What is Logistic Regression? - Logistic Regression Model Explained - AWS,” *Amazon Web Services, Inc.* Available: <https://aws.amazon.com/what-is/logistic-regression/> Accessed: Oct 18, 2024

[9] “What is random forest?,” *IBM*. Available: <https://www.ibm.com/topics/random-forest> Accessed: Oct 18, 2024

[10] S. Wiyono, D. S. Wibowo, and M. F. Hidayatullah, "Comparative Study of KNN, SVM, and Decision Tree Algorithm for Student’s Performance Prediction," *International Journal of Computing Science and Applied Mathematics*, vol. 8, no. 2, pp. 1–6, 2022.  
 Available: <https://iptek.its.ac.id/index.php/ijcsam/article/view/4360> Accessed: Oct 18, 2024

[11] P. T. Noi and M. Kappas, "Comparison of Random Forest, K-Nearest Neighbor, and Support Vector Machine Classifiers for Land Cover Classification Using Sentinel-2 Imagery," *MDPI Sensors*, vol. 18, no. 1, pp. 18-26, 2018.  
 Available: <https://www.mdpi.com/1424-8220/18/1/18> Accessed: Oct 18, 2024

[12] L. A. Demidova, "Two-Stage Hybrid Data Classifiers Based on SVM and kNN Algorithms," *MDPI Symmetry*, vol. 13, no. 4, pp. 615–630, 2021.  
 Available: <https://www.mdpi.com/2073-8994/13/4/615> Accessed: Oct 18, 2024

[13] J. B. Quinlan, "Induction of Decision Trees," *Machine Learning*, vol. 1, no. 1, pp. 81–106, 1986.  
 Available: <https://link.springer.com/article/10.1023/A:1022643204877> Accessed: Oct 18, 2024

[14] C. Cortes and V. Vapnik, "Support-Vector Networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.  
 Available: <https://link.springer.com/article/10.1007/BF00994018> Accessed: Oct 18, 2024

[15] K. R. Varma and N. Krishnan, "KNN vs SVM: A Comparative Study," *GeeksforGeeks*, 2020.  
 Available: <https://www.geeksforgeeks.org/svm-vs-knn-in-machine-learning/> Accessed: Oct 18, 2024

**Encryption**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Option*** | ***Key Length***  ***[80]*** | ***Encryption Speed***  ***[Opt]*** | ***Secure***  ***Low, Medium, High***  ***[Opt]*** | ***Tutorials for Implementation [Opt]*** | ***Known Attacks***  ***[Opt]*** | ***Time Required to Check all Possible Keys at 50 billion/Sec***  ***[Opt]*** | ***Raspberry PI Compatible***  ***With OpenSSL***  ***[Opt]*** |
| AES | 128/192/256 [1] | Fast [1] | High [1] | [5], [6] | Side Channel Attack [2] | 5x10^21 days [1] | Yes [10], [11] |
| DES | 56 [1] | Slow [1] | Low [1] | [6] | Brute Force Attack [2] | 400 days [1] | Yes  [12] |
| 3DES | 112/ 168 [1] | Slow [1] | Low [1] | [7] | Brute Force Attack, Chosen Plaintext, Known Plaintext [2] | 800 days [1] | Yes  [13] |
| Blowfish | 448 [1] | Fast [1] | Medium [1] | [8] | Dictionary Attack [2] | 3200 days [1] | Yes [14] |
| IDEA | 128 [3] | Slow [3] | Medium [3] | [9] | Meet in the Middle Attack [4] | N/A | Yes [15] |

Encryption Design Explanation:

DES was eliminated from consideration based on the key length not meeting our requirement (80). It also is not secure, and the brute force attack is a glaring vulnerability. 3DES is slow, insecure, and contains many known attacks. Therefore, 3DES is removed from consideration. IDEA is slow and speed is everything in this project. Thus, the only two remaining options are AES and Blowfish. Both are fast and meet the key length requirement. However, AES is more secure than IDEA, and the time required to check all the keys is substantially larger. After considering all of the options, we determined that AES will be the best option for encryption.

Encryption Sources

[1] S. Sari, "DES vs 3DES vs Blowfish vs AES," *Baeldung*, Baeldung. [Online]. Available: <https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes>

[2] A. Nurgaliyev and H. Wang, "Comparative study of symmetric cryptographic algorithms," *2021 5th International Conference on Cryptography, Security and Privacy (CSP)*, 2021, pp. 30-35. doi: 10.1109/CSP51677.2021.9634966. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9634966>.

[3] "AES vs IDEA," *This vs That*. [Online]. Available: <https://thisvsthat.io/aes-vs-idea>.

[4] "IDEA - International Data Encryption Algorithm," *TutorialsPoint*, [Online]. Available: <https://www.tutorialspoint.com/cryptography/idea_algorithm.htm>.

[5] W. Riddle, G. Quan, S. Salerno, E. Mendez, V. Formicola, N. El-Naga, and M. El-Haded, "AESPIE: Raspberry Pi AES performance evaluation using image encryption in C and Python," *in Advances in Artificial Intelligence, Software and Systems Engineering, Springer, 2024*, pp. 391-402. doi: 10.1007/978-3-031-40447-4\_30. [Online]. Available: <https://link.springer.com/content/pdf/10.1007/978-3-031-40447-4_30.pdf>.

[6] E. Fernando, D. Agustin, M. Irsan, D. F. Murad, H. Rohayani, and D. Sujana, "Performance comparison of symmetries encryption algorithm AES and DES with Raspberry Pi," *2019 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)*, 2019, pp. 54-58. doi: 10.1109/ICOMITEE.2019.8986122. [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8986122>.

[7] "Python DES Implementation," *GitHub Repository*. [Online]. Available: <https://gist.github.com/BlackRabbit-github/2924939>[8] "Encrypting data with the Blowfish algorithm," *Embedded.com*, Aspen Core Network. [Online]. Available: <https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/>.

[9] "Mastering IDEA Encryption Algorithm in Java: A Comprehensive Guide," *Coding Tech Room*, Code Room Tech. [Online]. Available: <https://codingtechroom.com/tutorial/java-mastering-idea-encryption-algorithm-in-java-a-comprehensive-guide>.

[10] I. Bull, "Tutorial: AES encryption and decryption with OpenSSL," EclipseSource, EclipseSource Jan. 17, 2017. [Online]. Available: <https://eclipsesource.com/blogs/2017/01/17/tutorial-aes-encryption-and-decryption-with-openssl/>.

[11] "EVP\_aes - OpenSSL," OpenSSL, 2018. [Online]. Available: <https://docs.openssl.org/1.1.1/man3/EVP_aes/>.

[12] "DES - OpenSSL," OpenSSL, 2016. [Online]. Available: <https://docs.openssl.org/1.0.2/man3/des/>.

[13] "Triple ECB mode - OpenSSL," OpenSSL, 2016. [Online]. Available: <https://docs.openssl.org/1.0.2/man3/des_modes/#triple-ecb-mode>.

[14] "Blowfish - OpenSSL," OpenSSL, 2016. [Online]. Available: <https://docs.openssl.org/1.0.2/man3/blowfish/>.

[15] "EVP\_CIPHER-IDEA - OpenSSL," OpenSSL, 2021. [Online]. Available: <https://docs.openssl.org/3.0/man7/EVP_CIPHER-IDEA/#algorithm-names>.