TWO-WAY SYMMETRIC ENCRYPTION FOR A SECURED MOBILE BASED YEAR BOOK GALLERY BASED ON LEMPEL-ZIV-WELCH COMPRESSION

Krishnah M. Lorejo[1], Zach Emmanuel C. Villamor[1], Jerome O. Abilay[2]
krishnahmunalem.lorejo@my.smciligan.edu.ph
ze.villamor@my.smciligan.edu.ph

[1]St. Michael's College of Iligan

ABSTRACT. The Mobile Yearbook Gallery at St. Michael's College addresses challenges in data security and multimedia file storage by utilizing two-way symmetric encryption and the Lempel-Ziv-Welch (LZW) compression algorithm. This system ensures data integrity during transmission and storage, making it efficient across devices due to its low processing requirements. The project employs HTML5, JavaScript, PHP, and CSS for front-end development, with MySQL for database management. The mobile app is developed using React.js and JavaScript, while security features are implemented in PHP alongside LZW compression. The system offers secure upload capabilities, encrypted data storage, and quick decryption and decompression services. Testing showed improved reliability and security without compromising file storage speed, achieving an average user satisfaction score of 83.75. Recommendations for improvement include granting alumni access to files, enhancing web hosting for user-friendliness, and optimizing the LZW algorithm to improve image storage efficiency and loading times. Ongoing development is suggested to adapt to user preferences.

Keywords: *Mobile Yearbook Gallery, Data security, Lempel-Ziv-Welch (LZW) compression, Two-way symmetric encryption, Data integrity, Secure upload, Encrypted storage, User satisfaction*

1. Introduction

The advancement of technology, especially in the current society, has not left the issue of capturing, storing, and sharing images by using applications in mobile phones. As discussed earlier, there has been a continued shift from the traditional 'yearbooks'' in schools, colleges, and other institutions to multimedia electronic ones, mainly due to the need to be elastic, interesting, and accessible. At St. Michael's College in Iligan City, it is the right moment to replace the old, less efficient yearbook system with a better, safer, and more efficient yearbook system that shall use the technology for the office of the Alumni Affairs Office.

For the security of this mobile-based yearbook gallery, it is recommended that two-way symmetric encryption be adopted, especially the AES algorithm; security is well enhanced since fields like images and user information are all encrypted to ensure that only the users with the decryption key are allowed access to the data.

In addition to security, the application will also focus on optimizing storage and performance. High-resolution images, which are a key component of yearbooks, can significantly increase the storage requirements and affect the application's performance. To mitigate this, the project will utilize the algorithm of Lempel-Ziv-Welch, a technique of lossless data compression that efficiently reduces the size of large pictures without compromising their quality [1]. The LZW algorithm is widely recognized for its effectiveness in compressing image files, making it an ideal choice for this application.

The integration of these advanced technologies is not merely a technical exercise but also a response to the evolving expectations of the digital- native generation. Students today demand seamless, intuitive, and secure digital experiences. By adopting a mobile application for the yearbook, St. Michael's College can meet these expectations and offer a platform that is accessible anytime and anywhere. This approach also aligns with the broader trend of digital transformation in education, where mobile apps are increasingly used to enhance learning

and engagement[2].

The study focuses on the need to have a secure, user-friendly, and efficient mobile-based yearbook application for St. Michael's College, Iligan City. Aiming to resolve the challenges of traditional yearbooks, the project will deliver a secure and efficient digital alternative through the use of encryption and compression. It enriches the yearbook with valuable alumni and staff contributions, while also establishing the college as a pioneer in educational digital transformation.

2. Objectives of the Study

The purpose of this study is to create secure and user friendly mobile based galleries for St. Michael's College's yearbook. The aim is to cut down on production time and costs by introducing digital solutions, eliminating paper, printing and binding. A mobile application will be used to access the yearbook gallery and privacy and security will be tested using two way symmetric encryption to ensure only authorized individuals can access the yearbook.

3. Methods

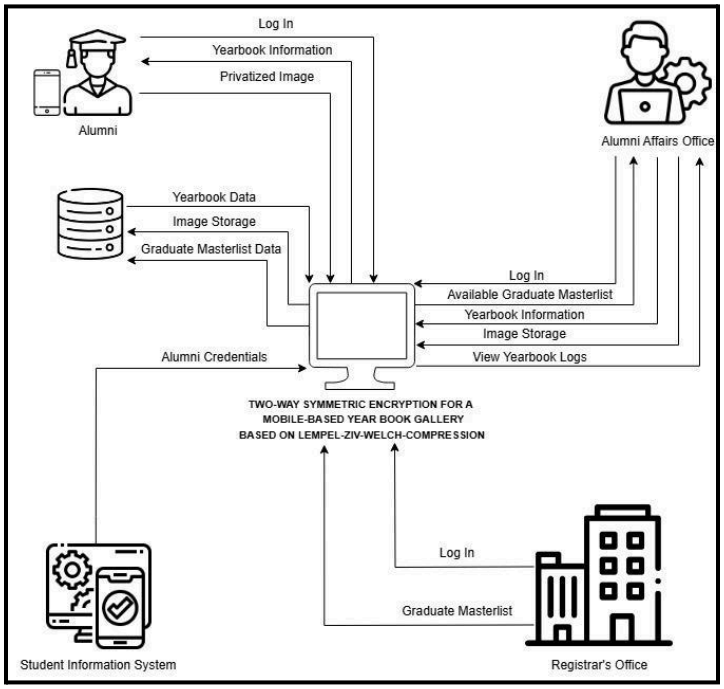

Figure 1. Conceptual Framework

It describes a conceptual framework for such a system that manages alumni information and yearbook reports. The admin of the system is the Alumni Affairs Office, which is responsible for managing the system and ensuring secure communication and data storage. Alumni entities can search and view yearbook information through the system. Secure communication and data retrieval is ensured by two-way symmetric encryption. The mobile-based yearbook gallery app hosts the yearbook gallery, accessible via mobile devices. The proposed project is bound with the Student Information System which contains alumni credentials and is retrieved through two-way symmetric encryption. Uploaded images from the Alumni Affairs Office are compressed using a specific code and stored in the database using the Lempel-Ziv-Welch Compression System. The passwords of users, including alumni, the office, and the registrar, are encrypted for security. The encrypted password from the database is decrypted by the system. The graduation master list is inputted by the registrar's office and the office obtains it to

be included in the yearbook. The yearbook database stores all data. The communication and data storage in the system is ensured to be secure and this in turn will give the users a secure and hassle-free experience.

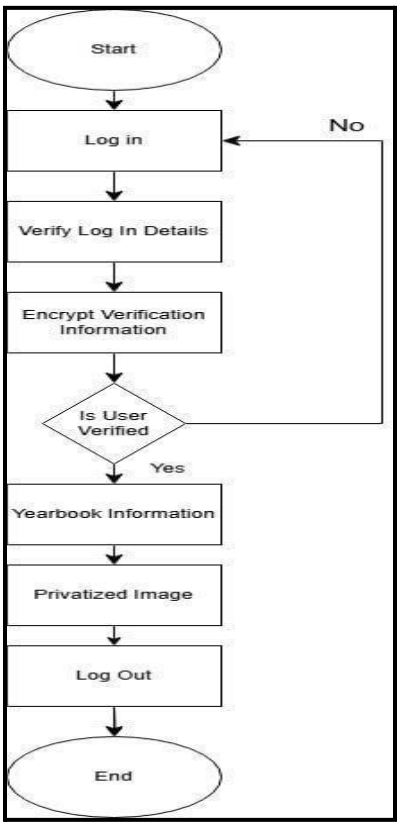

Figure 2. Process Flow Diagram

Figure 2 shows the process of logging in to the Alumni system involves a user's account name and password being authenticated. The information is encrypted for verification. If approved, the user can proceed to the next step. If not, the user returns to the login stage. Once validated, the user can search the yearbook freely. The yearbook can be viewed by the alumni. Finally, the process can be terminated by logging out.

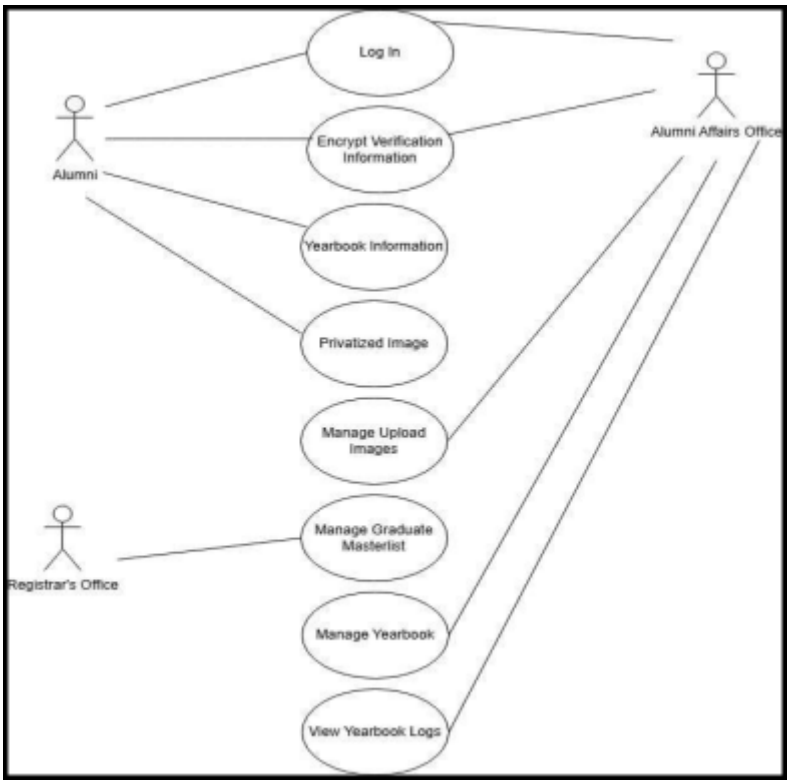

Figure 3. Use Case

The use case diagram shows the interactions between the actors such as alumni, Registrar's Office and Student Information System. Yearbooks can be accessed, alumni can authenticate themselves, and images can be privatized within their profiles. The graduate master list is handled by the Registrar's Office; they serve as the alumni credential, access, encryption verification, uploads, and report. The Student Information System helps in updating the student and alumni database for efficient yearbook completion. Alumni credentials are key functionality areas that include enhancing secure and efficient interactions between alumni and administrative offices.

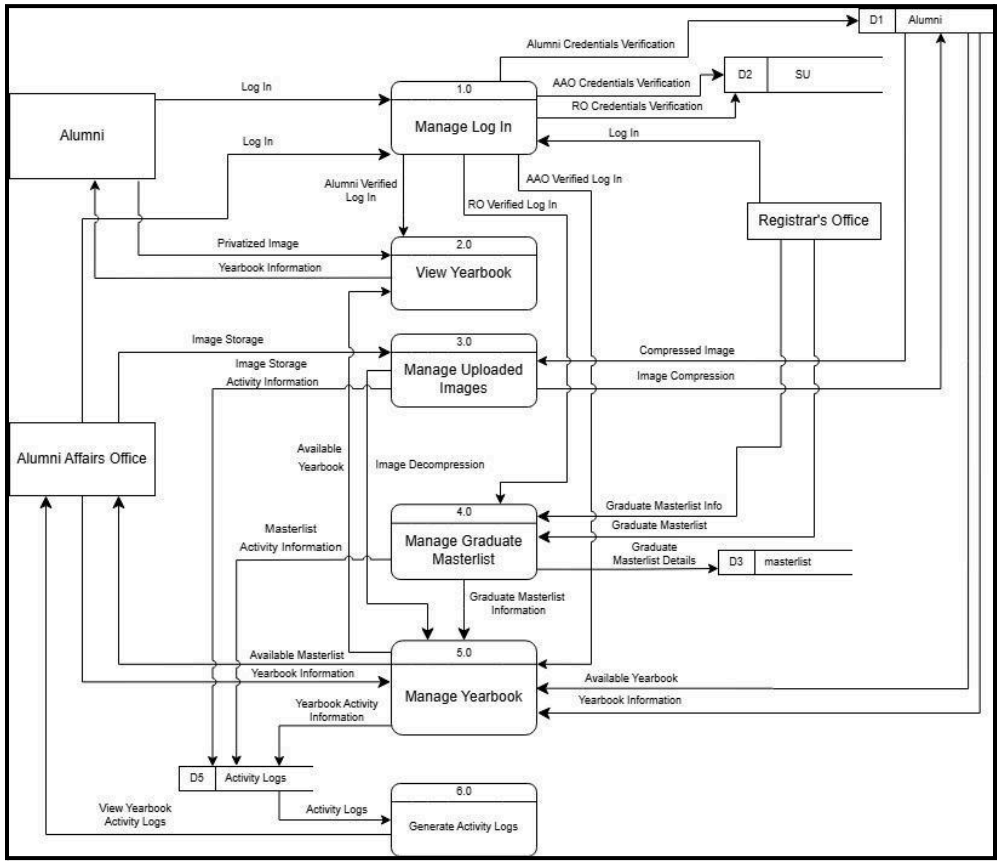

Figure 4. Level 0 Data Flow Diagram

Alumni yearbook data is managed by the system through various entities and databases. Available yearbooks can be accessed by alumni and privatized images can be accessed by alumni using SIS credentials. The Graduation Master List is populated with graduate details from the Registrar's Office for yearbook updates. The system is overseen by such office, which assigns codes to each alumnus, maintain images, yearbook information, and creates reports. It uses several databases such as Alumni Credentials, Alumni Affairs Office & Registrar Office Credentials, Graduate Masterlist, Yearbook, and Yearbook User Activity Logs. Uploaded images, graduate master list details and yearbook order are managed by the Alumni Affairs Office to ensure the safety and integrity of all data sent through the system. It also generates alumni credentials for user login.

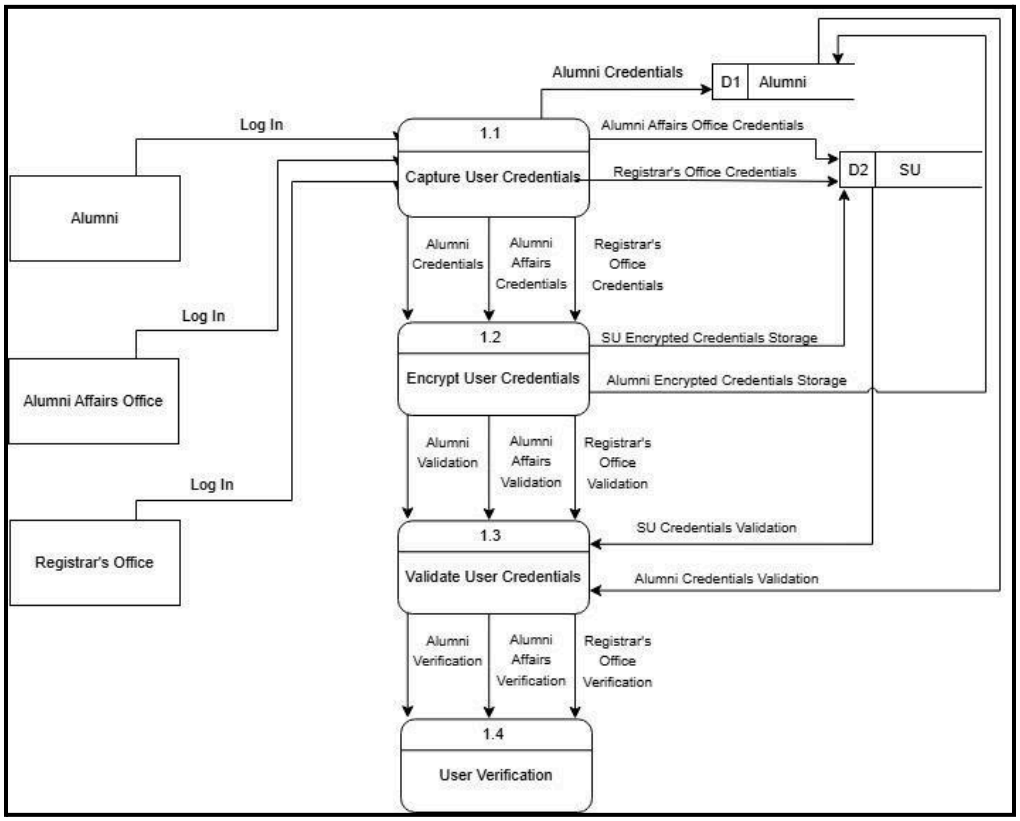

Figure 5. Level 1.0 Manage Login

The diagram describes a secure process for managing user credentials with three main entities: Alumni, Alumni Affairs Office, and Registrar's Office. These entities are captured by the system and the login credentials are encrypted for security and validated for authenticity. Then the system checks the credentials to see if it is working properly. Input credentials for each validation step are included in the data flow, as well as simple data stores (D1 for alumni credentials and D2 for the alumni affairs office and registrar). It allows it to control the stuffing and extraction of credentials to ensure that no one has access to vital information, including encryption, validation, and verification.

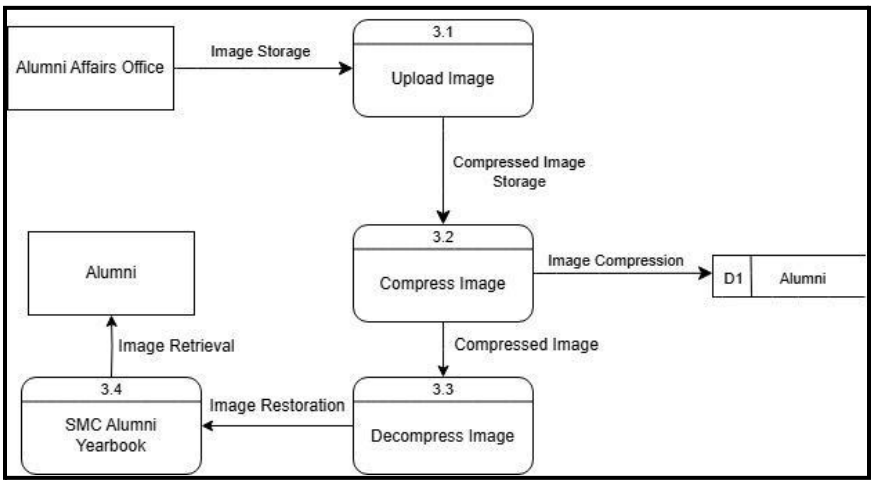

Figure 6. Level 1.0 Manage Uploaded Images

Images are uploaded by the Alumni Affairs Office and compressed for storage and efficiency. In process 3.2, the original image is compressed, and alumni can download it. The compressed images can later be decompressed, and users can access the original quality, as documented in the SMC Alumni Yearbook. This sequence guarantees good image management from upload to decompression.

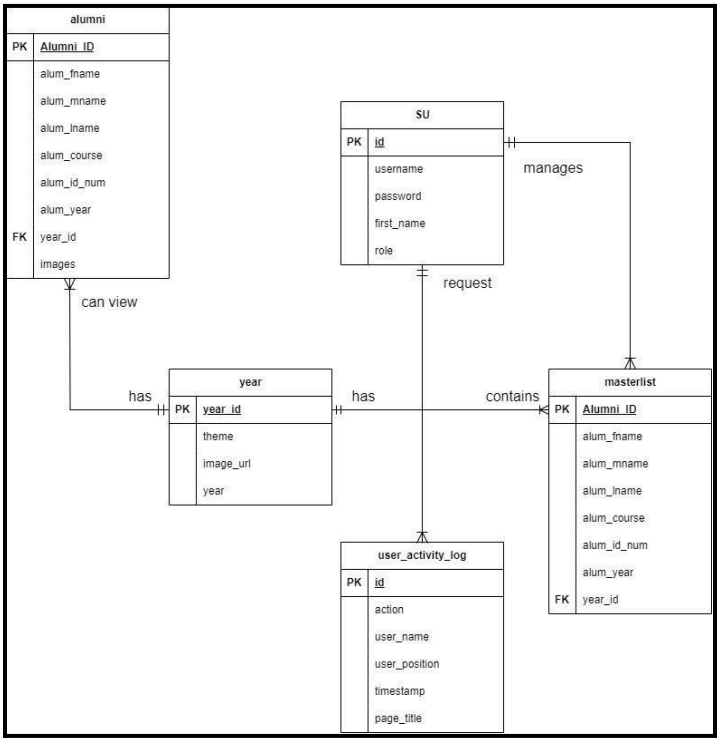

Figure 7. Entity Relationship Diagram

The Entity Relationship Diagram represents the implementation of entities in a system that focuses on alumni, yearbooks, and other relevant information. The Alumni entity includes several attributes, such as name, course, ID number, year graduated, and images. User-related data, having an ID key for unique identification of the entity, is owned by the SU (super user). The Year entity, which is measured by the primary key year_id, contains other specifics, year, themes, and image source related to yearbooks. The User Activity Log is an important entity in the system as it monitors the user interaction content from the site through the attributes action, user_name, user_position, time stamp, and the page title. The unique identifier of this entity is id. The Masterlist entity, which has close fields to Alumni, has the same primary key as Alumni, which is Alumni_ID. Alumni data, yearbooks, user management, and activity logs are dependent on relationships between these entities, and how these are related in a system enables the system to function effectively.

4. Results and Discussion

System Testing

The System Usability Scale is a Likert Scale which includes 10 questions which users of your mobile application will answer. Participants will rank each question from 1 to 5 based on how much they agree with the statement they are reading. 5 means they agree completely, 1 means they disagree vehemently.

Table 1

Results for the System Usability Scale Test

Indicators	Mean	Standard Deviation	Qualitative
I think that I would like to use this system frequently.	4.55	0.58	Very Often
I found the system unnecessarily complex.	1.65	0.96	Never
I thought the system was easy to use.	4.7	0.45	Very Often
I think that I would need the support of a technical person to be able to use this system.	2.05	1.43	Rarely
I found the various functions in this system were well integrated.	4.5	0.59	Very Often
I thought there was too much inconsistency in this system.	1.75	1.00	Never
I would imagine that most people would learn to use this system very quickly.	4.55	0.59	Very Often
I found the system very cumbersome to use.	1.6	0.96	Never
I felt very confident using the system.	4.65	0.48	Very Often
I needed to learn a lot of things before I could get going with this system.	1.7	0.56	Never

Overall Average: 83.75

Table 1 shows the results of all the scores from different respondents combined. Each of the question poses different meaning from negative to positive to mix in the differences of the system.

An overview of the method used in finding your SUS score. Users will have ranked each of the 10 template questions above from 1 to 5, based on their level of agreement. For each of the odd-numbered questions, subtract 1 from the score. For each of the even-numbered questions, subtract their value from 5. Take these new values that you have found and add up the total score. Then multiply this by 2.5. The result of all these tricky calculations is that you now have your score out of 100. This is NOT a percentage, but it is a clear way of seeing your score.

The System Usability Scale is not diagnostic and will not tell you what specific problems you face, but it will give you a red or green light to know how badly your usability needs work. The average System Usability Scale score is 68. If your score is under 68, then there are probably serious problems with your website usability, which you should address. If your score is above 68, then you can relax a little bit.

Here's an overview of how your scores should measure:

- 80.3 or higher is an A. People love your site and will recommend it to their friends
- 68 or thereabouts gets you a C. You are doing OK but could improve
- 51 or under gets you F. Make usability your priority now and fix this fast.

5. Conclusion

Conclusively, the mobile application, according to a mean score of 83.75 obtained over all users that used this study, showed its practicality and user cohesion.

This shows the overall average with 83.75, which shows that the study is excellent and can be relied upon. Note that for the purpose of enhancing performance as well as user satisfaction, there should still be continuous monitoring and development.

One must establish areas for growth specifically concerning compound system challenges, supervision, and the requirement of technical guidance. How the system adapts to changing user preferences and how it incorporates user feedback will determine its longevity in operation. Besides, Mobile Application Yearbook is very beneficial for St. Michael's College of Iligan since it enables providing the alumni and the school mobile access to their yearbook photos to further improve their nostalgic and school life, leading to alumni visiting the yearbook very often.

6. Recommendations

Based on the conclusions drawn, the following are the researchers' recommendations.

It is recommended to install AAO Access for AAO Admins in My.SMC. There is also no specific access granted to the AAO, and the system must be modified to allow for appropriate access to the AAO. A person who has an admin level at AAO should be able to manipulate the alumni records; this includes creating, modifying, and monitoring all records regarding alumni. This will assist in efficient working on alumni and strengthen the coordination with the alumni network.

The integration of the record of the SMC Basic Education Division (BED). As the system proposes the database on alumni, information from the Basic Education Division (BED) should also be included. This integration will enable tracking of all the alumni only for HED and BED to make sure that records from either of them are not lost.

Make use of the website to put in place an alumni tracking system. It is also important to incorporate tracked alumni on the website. Beneficial to the institution, this feature should help to manage alumni activity rates and their career advancement as well as improve alumni relations.
Upgrade the backend and web hosting regarding the web usability for clients; there is a need for better backend and website hosting to facilitate user access in the most efficient way. Optimizing hosting performance means the reduction of downtime, quick loading, and better usage of valuable resources in the system.
To enhance system security, it is suggested that a new layer of security be introduced to enhance the safety of the given data. Such a layer would enhance protection against leakage of sensitive data and unauthorized entry for the identity of alumni records.

Enhance the methodologies for the LZW algorithm for image compression. An idea for enhancing the existing LZW algorithm commonly utilized for compression of images is proposed here. It's possible to enhance the storage capacity's effectiveness within the proposed system and enhance the loading times of the images even more by decreasing the file sizes of the images even more.

7. References

[1] A. Anderson-Zorn and D. Long, "Digitize your yearbooks: Creating digital access while considering student privacy and other legal issues," *Journal of Contemporary Archival Studies*, vol. 8, no. 1, 2021. [Online]. Available: https://elischolar.library.yale.edu/jcas/vol8/iss1/14

[2] J. Bevers, *The Study of Symmetric and Asymmetric Key Encryptions*, University Honors College, Middle Tennessee State University, 2021. [Online]. Available: https://jewlscholar.mtsu.edu/handle/mtsu/6599

[3] O. Choudhari, M. Chopade, S. Chopde, and V. Ingle, "Hardware-based data compression using Lempel-Ziv-Welch algorithm," in *ICT for Competitive Strategies*. CRC Press, 2020.

[4] P. Dávila, N. Luis, and J. Miguelena, "Les annuaires scolaires: La richesse d'une source pour l'histoire de l'école et des élèves," *Encounters in Theory and History of Education*, vol. 21, pp. 253–273, 2020. [Online]. Available: https://doi.org/10.24908/encounters.v21i0.14404

[5] N. DiGiose, "Preserving memories: The timeless importance of yearbooks," *In Focus*, May 9, 2023. [Online]. Available: https://www.irvinsimon.com/blog/why-yearbooks-are-important-to-your-school-community/

[6] Fiona, "Case study: The place of yearbooks in an increasingly online world," *Imageseven*, Nov. 14, 2021. [Online]. Available: https://www.imageseven.com.au/case-study-the-place-of-yearbooks-in-an-increasingly-online-world/

[7] T. C. G. and J. Devi, "A study and overview of the mobile app development industry," *International Journal of Applied Engineering and Management Letters (IJAEML)*, vol. 5, no. 1, 2021.

[8] J. Gardner, Y. Feng, K. Reiman, Z. Lin, A. Jain, and N. Sadeh, "Helping mobile application developers create accurate privacy labels," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022, pp. 212–230. [Online]. Available: https://doi.org/10.1109/EuroSPW55150.2022.00028

[9] F. Hardy, "Pages to screen: Digitalized yearbook with chatbox and gallery," *International Journal of Science and Applied Information Technology*, vol. 13, no. 1, pp. 1–5, 2024. [Online]. Available: https://doi.org/10.30534/ijsait/2024/011312024

[10] Z. Huang and M. Benyoucef, "An empirical study of mobile application usability: A unified hierarchical approach," *International Journal of Human–Computer Interaction*, vol. 39, no. 13, pp. 2624–2643, 2023. [Online]. Available: https://doi.org/10.1080/10447318.2022.2082021

[11] N. A. Kadim, S. K. Guirguis, and H. A. Elsayed, "Discrete shearlet transform and Lempel-Ziv Welch coding for lossless fingerprint image compression," *Journal of Computer Science*, vol. 20, no. 5, pp. 564–573, 2024. [Online]. Available: https://doi.org/10.3844/jcssp.2024.564.573

[12] A. Kadir, A. Habibi Lashkari, and M. Firoozjaei, *Mobile Application Security*, 2024, pp. 89–101. [Online]. Available: https://doi.org/10.1007/978-3-031-48865-8_6

[13] Ş. M. Kaya and M. A. Akçay, "Image compression performance comparison of RLE and LZV algorithms for effective big data management: A case study," *Anadolu Bil Meslek Yüksekokulu Dergisi*, vol. 17, no. 66, 2023.

[14] S. M. Malode and N. Rajurkar, "Development of online college yearbook," *International Journal of Computer Science and Mobile Computing*, vol. 11, no. 3, pp. 31–36, 2022. [Online]. Available: https://doi.org/10.47760/ijcsmc.2022.v11i03.004

[15] M. Nadeem, A. Arshad, S. Riaz, S. Zahra, S. S. Band, and A. Mosavi, "Two-layer symmetric cryptography algorithm for protecting data from attacks," *Computers, Materials and Continua*, vol. 74, pp. 2625–2640, 2022. [Online]. Available: https://doi.org/10.32604/cmc.2023.030899

[16] D. Oliveira, L. Pedro, and C. Santos, "The use of mobile applications in higher education classrooms: An exploratory measuring approach in the University of Aveiro," *Education Sciences*, vol. 11, no. 9, 2021. [Online]. Available: https://doi.org/10.3390/educsci11090484

[17] R. E. H. S. Rajendra, T. V. Reddy, B. L. N. Murthy, J. S. Bhagavan, S. S, and S. S. Aravinth, "Secure encryption framework for multi-cloud environments: Leveraging symmetric and asymmetric encryption," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2023, pp. 1493–1500. [Online]. Available: https://doi.org/10.1109/ICECA58529.2023.10394865

[18] A. C. M. Review, "Social media use and yearbooks," *College Media Review*, vol. 57, Feb. 25, 2020. [Online]. Available: https://cmreview.org/social-media-yearbooks/

[19] S. Rocque, "Evaluating the effectiveness of mobile applications in enhancing learning and development," *International Journal of Innovative Technologies in Social Science*, Sep. 30, 2022. [Online]. Available: https://doi.org/10.31435/rsglobal_ijitss/30092022/7847

[20] B. P. Singh and M. Madhusudhan, "Mobile apps–based applications in libraries and information centers: A systematic review of the literature and future research agendas," *International Journal of Librarianship*, vol. 8, no. 3, 2023. [Online]. Available: https://doi.org/10.23974/ijol.2023.vol8.3.294

[21] Q. Zhang, "An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption," in *2021 2nd International Conference on Computing and Data Science (CDS)*, 2021, pp. 616–622. [Online]. Available: https://doi.org/10.1109/CDS52072.2021.00111