Developing a secured image file management system using modified AES

Heidilyn V. Gamido[1], Marlon V. Gamido[2], Ariel M. Sison[3]
[1,2]Tarlac State University, Tarlac City, Philippines
[3]Emilio Aguinaldo College, Manila, Philippines

Article Info

Article history:

Received Aug 30, 2018
Revised Nov 22, 2018
Accepted Jul 10, 2019

Keywords:

AES
Encryption
File management system
Image file encryption

ABSTRACT

Images are a means to share and convey relevant data in today's digital world. This paper presents an image file management system to provide a platform for distributing and viewing images in a secured manner. The shared image files are stored in the server in an encrypted manner to provide additional security to the owner of the file. A modified AES algorithm using bit permutation was used to encrypt the image files. Based on the experimental result, image files were successfully encrypted in the server and can only be decrypted by the intended recipient of the file providing an efficient and reliable way of exchanging images.

Corresponding Author:

Heidilyn V. Gamido,
Tarlac State University,
Tarlac City, Philippines.
Email: htvgamido@tsu.edu.ph

1. INTRODUCTION

In today's digital world, the use of images as a means to disseminate and convey relevant information becomes a normal practice [1, 2]. With the advancement of technologies, the continuing increase in information sharing using images imposes challenges in capturing, displaying, sharing and archiving image as well as prone to security threats [3]. Image sharing is important in the fields of medical processing [4, 5], remote sensing [6], government documents [7], military and other similar fields [8, 9].

The common practice of using physical storage like CDs and USB flash drives are used to transport images to hand-carry digital images from one destination to the next. This practice may be convenient if the recipient is near to the sender. Another problem that may arise from transporting images using portable devices is the accidental write or erase processes [10], vulnerability to virus [11] and hardware failure.

If an organization has an extensive range of images captured and shared within the organization, a system is needed to manage and secure the collection of image files. Development of an Image File Management System (IFMS) will provide a platform to share, distribute and view images in a secured manner by encrypting these files in the central storage. The implementation of an image management system will improve internal communication and can be used in organizations such as clinics, hospitals, schools, and government institutions and will increase staff efficiency and process workflow.

The objective of this paper is to introduce an image file management system that can be used to store, view and share images. The use of the modified AES provides an additional level of security to the sender or owner of the image. The file to be shared is encrypted using the modified AES algorithm, providing additional protection to the owner of the image. The encrypted image is received, viewed and downloaded only by the intended recipient. Encrypting a file in the server provides an efficient and reliable way of exchanging and sharing images for transmission over a network infrastructure [12].

2. REVIEW OF RELATED LITERATURE

This section presents some available file-sharing applications like documents management system, medical image management system and image management system.

2.1. Electronic document management systems (EDMS)

An Electronic Document Management System prepares the documents for uploading and sharing the document with different users and ends with archiving said document [13]. Due to bulk use of documents in several types, the use of EDMS in Universities also provide a various advantage in reducing the operational cost in producing, sharing, and copying the document. EDMS also shortened the time in document accessing and archiving, provided higher work efficiency because multiple users are enabled to work on the same document and connection can be established easily between different documents [13].

An electronic management system (EDMS) presented by [14] showed an increase in the efficiency of an organization by reducing cost and increasing the result. EDMS provided more income to an organization because of lesser spending cost in paper documents, overhead staff time and changes corporate culture.

An implementation of EDMS, a system for the management of documents, provided an advantage in the administrative work in government [7]. The use of such management system increased the operational effectiveness of governments on a daily basis such as document storage and retrieval, workflow facilities, auditing, searching, and publishing.

2.2. Medical image management system (MIMS)

The medical image management systems [15] enable the transmission of chest x-ray images in a hospital. The implementation of MIMS in hospital replaces the conventional equipment and film-handling schemes in hospitals. This system acquires medical images, transmit them, store and archive them using magnetic disk and viewed in a physician and radiologist station. The MIMS provided the convenience of having images available earlier, lessening the need to visit the radiology department. The exchange and sharing of medical images provided compelling values such as cost reduction, improved collaboration and patient care which increased patient satisfaction the use of such system streamlining an important process that has been facilitated with the use of physical devices or any insecure methods of communication [16].

2.3. Picture/image library software

The paper of [17] described the role of software like SharePoint Foundation 2010 Picture Library in locating and creating photo database. The implementation of such software provided searchable photo database and provided success to both end users and contributors because photos are no longer missing and users spend less time searching appropriate photos. With this, the developed system is also capable of searching the database of shared images for easy retrieval of images.

2.4. Image management system

The University of Duckham implements an Image Management System to help departments, colleges, and units across the University access existing University-wide images, and to provide users of the system the option to upload and store their images, creating a central source for all University images [18]. The proposed system is a LAN-based system used implemented in a University to share image files across the organization, and the files are encrypted in the server side. The user also has the option to select the recipient/s who will receive, view, and download the image file.

3. PROPOSED METHOD

This section explains the methods used in developing the system. Figure 1 shows the operational framework of the proposed IFMS. Users of the system log in using their correct credentials-username and password. The sender of the image selects the image file to be shared to intended recipients. The file will be encrypted using the Modified AES algorithm [19] shown in Figure 2, and the encrypted file is stored at the server. The shared file is received once the recipient logs in the system, and the recipient can view the decrypted file once the file is clicked. The recipient can save the decrypted image in another location if the recipient needs to use it for other purposes.

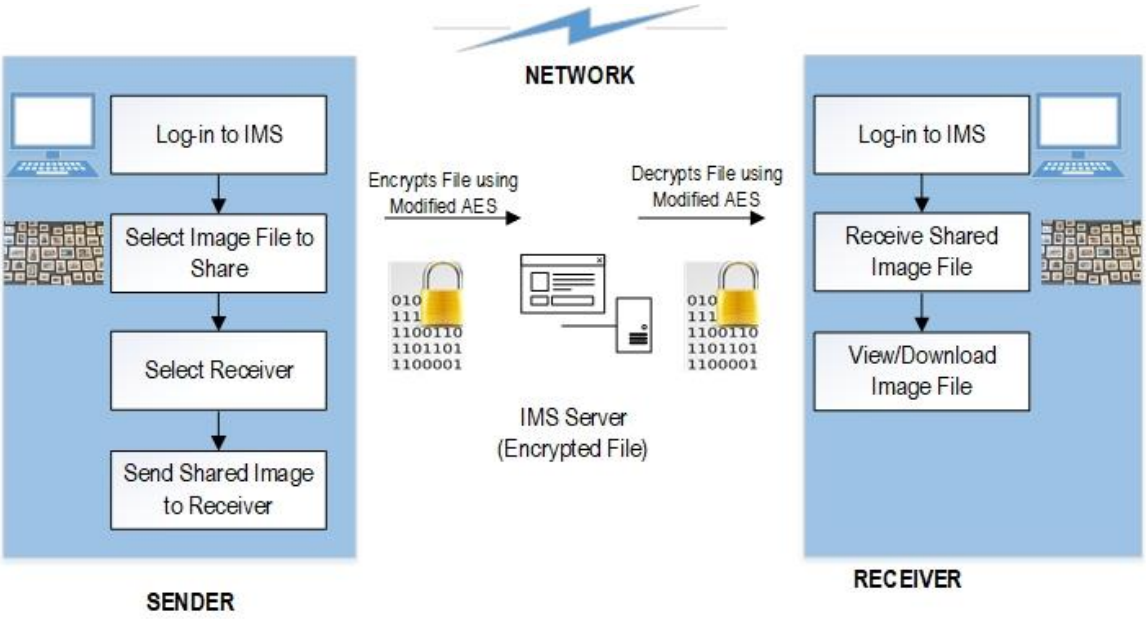

NETWORK
Log-in to IMS
Select Image File to Share
Select Receiver
Send Shared Image to Receiver
SENDER
Encrypts File using Modified AES
Decrypts File using Modified AES
010 111 1100110 1101101 1100001
IMS Server (Encrypted File)
Log-in to IMS
Receive Shared Image File
View/Download Image File
RECEIVER

Figure 1. Operational design of the proposed application

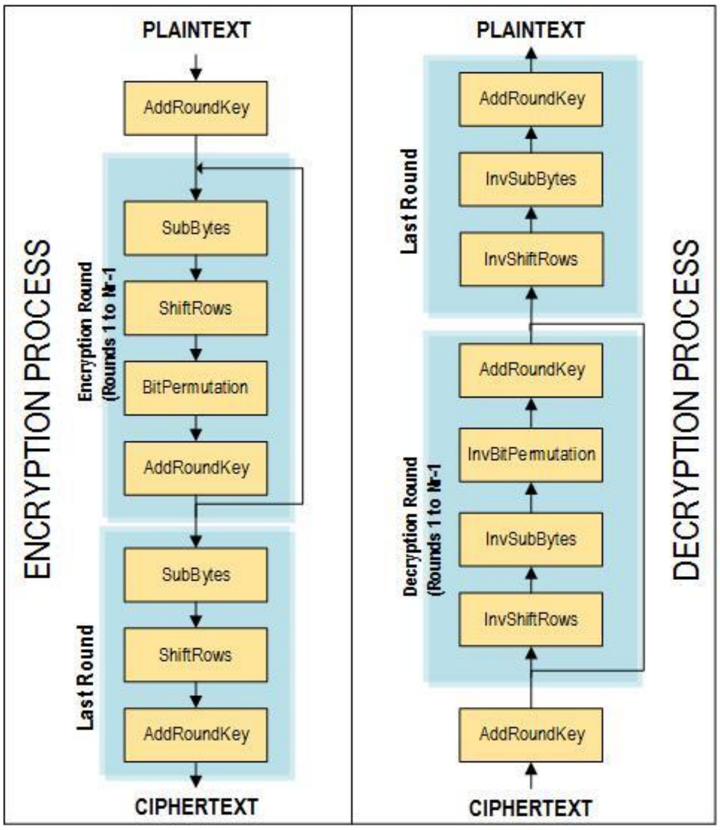


Figure 2. Proposed modified AES algorithm

3.1. Modified AES algorithm

A modified AES algorithm [19] is used to encrypt the files to secure the image file in the server. Bit Permutation Transformation replaces the MixColumns Transformation in AES. The bit permutation transformation does not have complex mathematical computation [20] but only involves shifting of the position of bits of every state. To perform the bit permutation for the encryption process, the state in Shift Rows is carried out in this transformation and follow the steps below.

a. Take the state value per column, for example, column 0.

b. Column 0 has four rows, and each state in (x,0) is composed of 8 bits resulting in a 4x8 matrix. ((x,0), b) represents the row, column and bit number in each state.

c. The 4x8 matrix can also be represented by a

d. Next step is to get the transpose of each block matrix.

e. The value of a’(x,y), is a row-wise concatenation of the bit values of the transposed block, where x=column value in ShiftRows and y=block number in the 4x2 partitioned matrix.

4. RESULTS AND ANALYSIS

4.1. System development

The Image File Management System was developed using Visual Studio C#, and the system database was designed using MS SQL 2016. The developed system was tested in the local area network of Tarlac State University.

4.2. System module

4.2.1. Login module

To be able to access the designed system, users need to register to the system. Registration of users is to be performed by the administrator of the system. Correct credentials such as username and password are to be supplied to use the system. Registered users can share, search, view, download files from the system show in Figure 4.

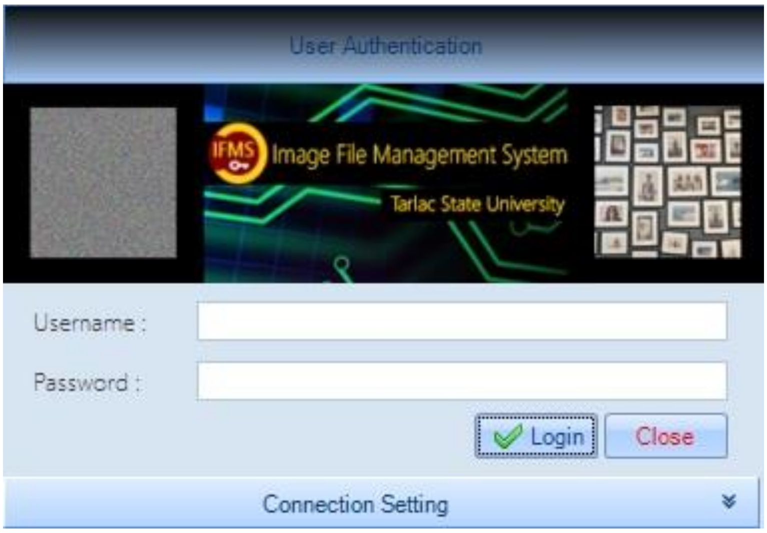
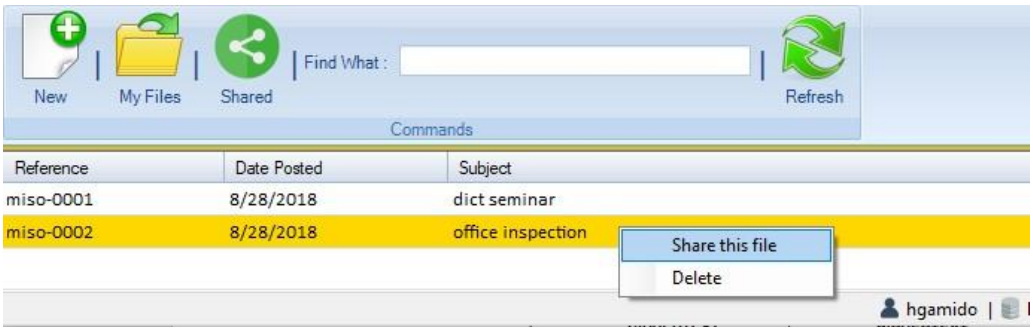


Figure 4. Login module

4.2.2. File module

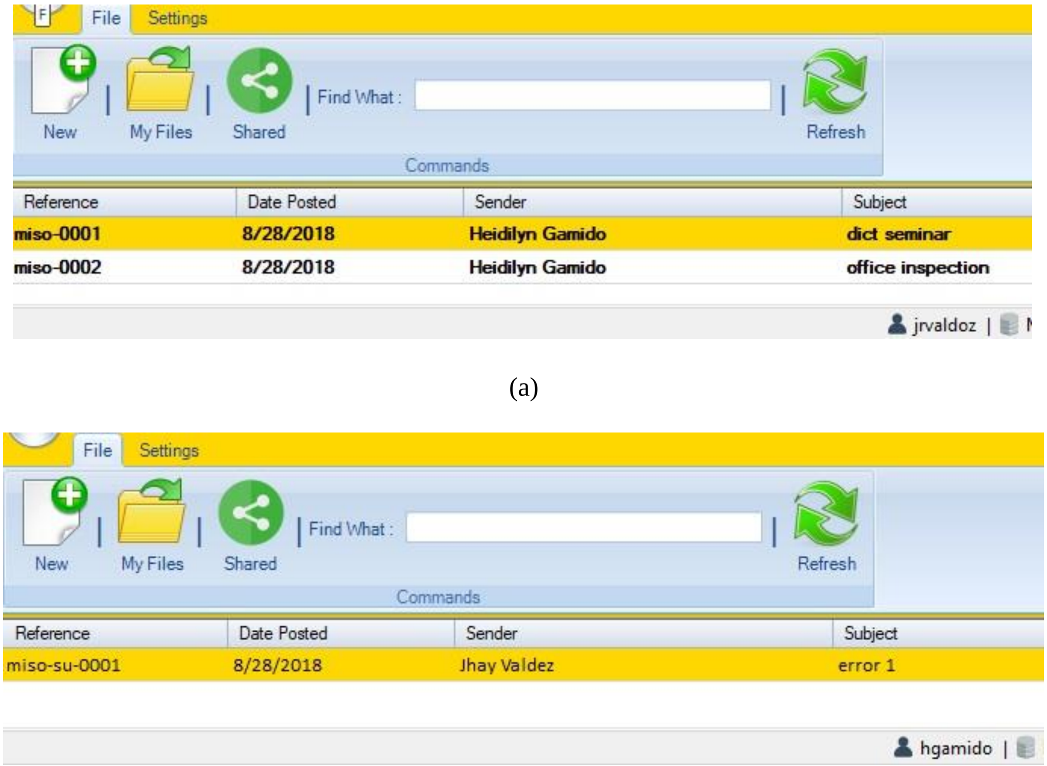
The file module enables the user to add a file, view the uploaded files and search for files. The files from this module can be shared by the owner to intended users show in Figure 5.



Reference	Date Posted	Subject
miso-0001	8/28/2018	dict seminar
miso-0002	8/28/2018	office inspection

Figure 5. Sharing image file

Once the sender clicks the share this file menu, he selects the desired recipient of the file based from the group settings (for multiple sending) or to an individual user. Figure 6(a), Figure 6(b) shows that the intended recipient has received the shared file once the user logs into the system. A highlighted message means that the receiver has not opened the file (Figure 6a). If the receiver has opened the message, the highlighted message is removed (Figure 6b).



Reference	Date Posted	Sender	Subject
miso-0001	8/28/2018	Heidilyn Gamido	dict seminar
miso-0002	8/28/2018	Heidilyn Gamido	office inspection

(a)

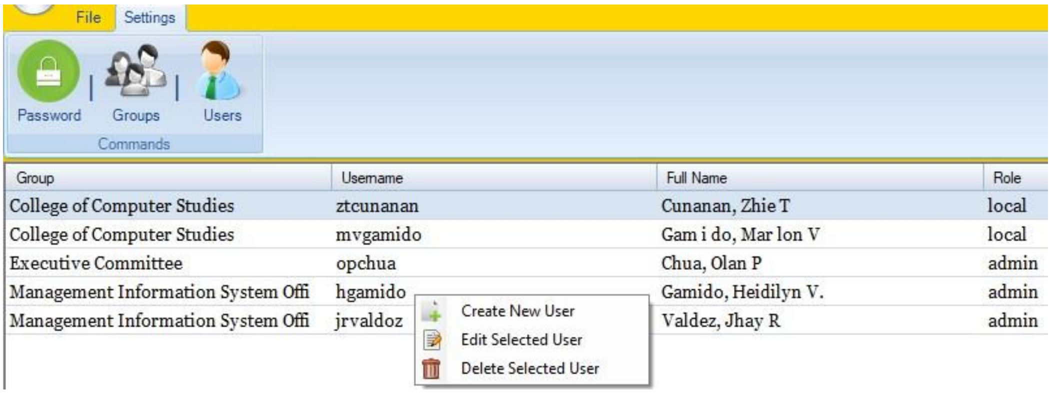
Reference	Date Posted	Sender	Subject
miso-su-0001	8/28/2018	Jhay Valdez	error 1

(b)

Figure 6. (a) Received shared file, (b) Received shared file

4.2.3. Setup module

The setup module is used to add users, group and modify the user information such as password, name, and role show in Figure 7.

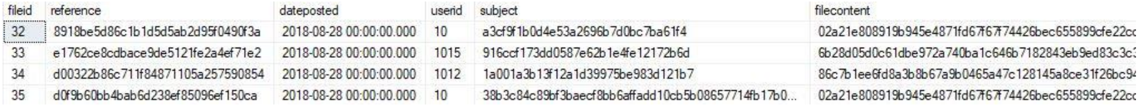


Group	Username	Full Name	Role
College of Computer Studies	ztcunanan	Cunanan, Zhie T	local
College of Computer Studies	mvgamido	Gam i do, Mar lon V	local
Executive Committee	opchua	Chua, Olan P	admin
Management Information System Offi	hgamido	Gamido, Heidilyn V.	admin
Management Information System Offi	jrvaldoz	Valdez, Jhay R	admin

Figure 7. Setup module

4.2.4. Encrypted database

Figure 8 shows the database of the IFMS. Fields like a reference, subject, and the file content have been encrypted to provide additional security to the file. The fields are encrypted using the modified AES algorithm.



fileid	reference	dateposted	userid	subject	filecontent
32	8918be5d86c1b1d5d5ab2d95f0490f3a	2018-08-28 00:00:00.000	10	a3cf9f1b0d4e53a2696b7d0bc7ba61f4	02a21e808919b945e4871fd67f67f74426bec655899cfe22cc
33	e1762ce8cdbace9de5121fe2a4ef71e2	2018-08-28 00:00:00.000	1015	916ccf173dd0587e62b1e4fe12172b6d	6b28d05d0c61dbe972a740ba1c646b7182843eb9ed83c3c
34	d00322b86c711f84871105a257590854	2018-08-28 00:00:00.000	1012	1a001a3b13f12a1d39975be983d121b7	86c7b1ee6fd8a3b8b67a9b0465a47c128145a8ce31f26bc9
35	d0f9b60bb4bab6d238ef85096ef150ca	2018-08-28 00:00:00.000	10	38b3c84c89bf3baecf8bb6affadd10cb5b08657714fb17b0...	02a21e808919b945e4871fd67f67f74426bec655899cfe22cc

Figure 8. Encrypted database

5. CONCLUSION

This paper presented an image file management system to provide an avenue for sharing, distributing and viewing image files in a secured manner. A modified AES algorithm was used to encrypt the file and other relevant information to provide additional security to the owner of the file. The image file management system has successfully shared and distributed files among users and has successfully encrypted the file in the server using the modified algorithm. In the future, other file types, such as a document, audio, and video, can be used to share and distribute using the application.

ACKNOWLEDGMENT

The authors gratefully acknowledge the Commission on Higher Education, K-12 Project Management Unit, Philippines for the scholarship and the Tarlac State University Management Information Systems Office for the completion of the research.

REFERENCES

[1] D. W. Cromey, “Digital Images Are Data: And Should Be Treated as Such,” in Methods in Molecular Biology, vol. 931, no. 28, D. J. Taatjes and J. Roth, Eds. Totowa, NJ: Humana Press, 2012, pp. 1–27.

[2] A. Yudhana, Sunardi, and S. Saifullah, “Segmentation comparing eggs watermarking image and original image,” *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 1, pp. 47–53, 2017.

[3] Shivaputra, H. Sheshadri, and V. Lokesha, “A Naïve Visual Cryptographic Algorithm for the Transfer of Compressed Medical Images,” *Bulletin of Electrical Engineering and Informatics*, vol. 5, no. 3, pp. 347–365, 2016.

[4] K. J.-W. Kim T., Heo E., Lee M., Kim J., Yoo S., Kim S., Lee K., “Medical image exchange and sharing between heterogeneous picture archiving and communication systems based upon international standard: pilot implementation” *15th Int. HL7 Interoperability Conf.*, pp. 37–42, 2015.

[5] R. Pienaar et al., “CHIPS-A Service for Collecting, Organizing, Processing, and Sharing Medical Image Data in the Cloud,” in *Data Management and Analytics for Medicine and Healthcare*, 2017, pp. 29–35.

[6] L. Zhou, N. Chen, Z. Chen, and C. Xing, “ROSCC: An Efficient Remote Sensing Observation-Sharing Method Based on Cloud Computing for Soil Moisture Mapping in Precision Agriculture,” *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 9, no. 12, pp. 5588–5598, 2016.

[7] H. Abdulkadhim, M. Bahari, A. Bakri, and W. Ismail, "A research framework of electronic document management systems (EDMS) implementation process in government," *J. Theor. Appl. Inf. Technol*., vol. 81, 2015.

[8] P. K. Das, P. Kumar, and M. Sreenivasulu, "Image Cryptography : A Survey towards its Growth," *Adv. Electron. Electr. Eng. Res. India Publ*., vol. 4, no. 2, pp. 179–184, 2014.

[9] Q. Zhang and A. Qunding, "Digital image encryption based on Advanced Encryption Standard(AES) algorithm," *5th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC 2015*, pp. 1218–1221, 2015.

[10] O. Nekhayenko, "Preserving and accessing content stored on USB-flash-drives–a TIB workflow*," Grey J*., vol. 14, no. 2, pp. 95–101, 2017.

[11] A. Cohen and N. Nissim, "Trusted Detection of Ransomware in a Private Cloud Using Machine Learning Methods Leveraging Meta-Features from Volatile Memory," *Expert Syst. Appl.*, 2018.

[12] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Securing Electronic Medical Records Using Modified Blowfish Algorithm," *Indones. J. Electr. Eng. Informatics*, vol. 6, no. 3, pp. 309–316, 2018.

[13] M. Başıbüyük and A. Ergüzen, "Electronic Document Management System for Kırıkkale University*," Unified J. Comput. Sci. Res. Unif. J. Comp. Sci. Res*, vol. 1, no. 2, pp. 8–15, 2015.

[14] I. N. Burtylev, K. V Mokhun, Y. V Bodnya, and D. N. Yukhnevich, "Development of Electronic Document Management Systems: Advantage and Efficiency," *Sci. Technol.* March, pp. 1–9, 2013.

[15] S. B. Seshadri, R. Arenson, S. Khalsa, I. Brikman, and F. van der Voorde, "Prototype Medical Image Management System (MIMS) at the University of Pennsylvania: Software Design Considerations," *J. Digit. Imaging*, vol. 16, no. 1, pp. 96–102, Mar. 2003.

[16] A. Vreeland et al., "Considerations for Exchanging and Sharing Medical Images for Improved Collaboration and Patient Care: HIMSS-SIIM Collaborative White Paper," *J. Digit. Imaging*, vol. 29, no. 5, pp. 547–558, 2016.

[17] T. Harron, "SharePoint picture library as a searchable photo database in a small library: a program description," *J. Can. Heal. Libr. Assoc. / J. l'Association des bibliothèques la santé du Canada*, vol. 36, no. 1, p. 20, 2015.

[18] "Image Management System-Durham University." [Online]. Available: https://www.dur.ac.uk/marketingandcommunications/marketing/images/. [Accessed: 27-Jul-2018].

[19] H. V. Gamido, A. M. Sison, and R. P. Medina, "Modified AES for Text and Image Encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 11, no. 3, pp. 942–948, 2018.

[20] H. V. Gamido, A. M. Sison, and R. P. Medina, "Implementation of Modified AES as Image Encryption Scheme," *Indonesian Journal of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 301–308, 2018.

BIOGRAPHIES OF AUTHORS

Heidilyn V. Gamido is a graduate of Doctor in Information Technology at Technological Institute of the Philippines, Quezon City under the CHED K-12 Transition Program Scholarship. She obtained her Masters of Engineering major in Information and Communications in 2006 at Pai Chai University, Daejeon South Korea on a scholarship. She finished her BS Information Technology at Saint Louis University, Baguio City Philippines in 2002. She is an Associate Professor of Tarlac State University-College of Computer Studies and designated as the Director of the Management of Information Systems Office. Her research interests include data security, image processing, and information system.

Marlon V. Gamido is the Dean of College of Computer Studies in Tarlac State University. He holds a degree in MS in Information Technology from Hannam University, Daejeon Korea on CHED Scholarship. He is currently pursuing his PhD in Educational Management at TSU. He is also a registered Electrical Engineer. His research interests include security and project management.

Ariel M. Sison earned his Doctor in Information Technology at the Technological Institute of the Philippines Quezon City in 2013 and graduated with Highest Honors. He took up his master's degree in computer science at De La Salle University Manila in 2006 and obtained the BS Computer Science at Emilio Aguinaldo College Manila in 1994. He is currently the dean, School of Computer Studies, Emilio Aguinaldo College Manila. His research interests include data mining and data security. Dr. Sison is a member of International Association of Engineers (IAENG), Philippine Society of IT Educators and Computing Society of the Philippines. Currently, he is a Technical Committee Member of International Academy, Research, and Industry Association (IARIA) for International Conference on Systems (ICONS).