Implementing a Visual Cryptography Scheme for Password Authentication

Louise Gabrielle L. Talip and Joseph Anthony C. Hermocilla

I. Introduction

A. Background of the Study

Filipinos are known to be one of the most active individuals on the internet across the globe, specifically in social media platforms such as Facebook, Twitter, and Instagram where users must register and create personal accounts in order for them to use the platform. The Philippines has ranked at the top for average daily time spent using social media according to the 2021 report from DataReportal [1]. Despite being digitally active, Filipinos are also known for poor security practices on the internet, with a consensus that security is only secondary over having connectivity even in public networks [2]. The popularity of the usage of these platforms alongside the absence of cybersecurity awareness and literacy produces a new avenue for malicious attackers to take advantage. Especially since the transition to the digital space due to the coronavirus disease in 2019, Filipinos are more vulnerable to attacks than ever.

Cryptography is a mechanism to protect messages from people who are not authorized to read it by translating plain text to an encoded message [3]. As explained by Elprocus [4], it is one of the primary techniques used in creating a secure line of communication for various digital technologies such as web, mobile, or desktop applications and physical devices such as automated teller machines, printers, and global positioning systems. The message transmitted by the sender is secured via an encoder (encrypting) and the encoded message is sent to the receiver, who has the only capability or access to decode the message (decrypting). Ideally, the message should not be intercepted or decoded by any unauthorized individual or application program. There are different mechanisms of cryptography that are applied in the authentication of web applications, with the Advanced Encryption Standard (AES) as the most widely used.

Visual Cryptography, on the other hand, is one of the cryptographic techniques that is used to encrypt images. One of the notable characteristics of visual cryptography is its reliance on human interaction. The secret image can be broken into two or more parts called shares and is distributed to the people who need to keep the secret. The only way in which the secret can be revealed again is by having all shares present superimposed in a specific way [5]. Once the image is decrypted, there is no need for computer interaction as human vision is needed to understand the decrypted message or image, a well-recognized example of which is CAPTCHA based authentication. Authentication that relies only on the user's own and exclusive interaction could increase the robustness and security of a user's personal account on the internet, and thus, is the primary subject of this study. Furthermore, this study will solely focus on the feasibility and reliability of a registration and login system that utilizes visual cryptography.

B. Statement of the Problem

Cybersecurity has been an increasingly prevalent issue in the Philippines as more people own smartphones, laptops, and other electronic devices that have the capacity to connect to the internet. According to DataReportal [1], as of January 2021, there are around 89 million social media users in the Philippines out of the 110.3 million population of the country, which is a drastic increase of 16 million or 22% between 2020 and 2021. However, in an Internet security awareness survey paper conducted by Omorog and Medina [2], many of the respondents use free WiFi access points in public establishments to use Internet services such as emailing and downloading which are known to be more susceptible to cyber attacks and data collection. During the start of the 2020 pandemic alone, the Cybercrime Division of the National Bureau of Investigation has reported a 200% increase of phishing scams across the country [6]. These scams exploit vulnerable and digitally illiterate individuals by acting as a trusted entity through fake websites or formally written emails and texts. Because of this, they are able to lure people into clicking fraudulent links or giving out sensitive data such as usernames, passwords, or credit card information. According to Kaspersky [7], an internet security firm, there has been a 25% increase in the number of password stealers in the Philippines during the first quarter of 2021, with a total of 55,597 attacks, compared to the 45,373 attacks in 2020 during the same period.

Today, many authenticated websites, or websites that require user registration and login, use non-visual means of authentication such as string usernames and passwords. This is more prone to certain malicious attacks for two main reasons:

1) Popular password attacks such as Trojan horse programs, brute-force attacks, key logging, and packet sniffing can easily crack weak string-based passwords, which is prevalent among many Filipinos according to the global analytics software company FICO in 2020 [8].

Presented to the Faculty of the Institute of Computer Science, University of the Philippines Los Baños in partial fulfillment of the requirements for the Degree of Bachelor of Science in Computer Science

2) Creating a legitimate-looking copy of a trusted institution's website, which is often the primary method of stealing sensitive data, is very accessible and uncomplicated to many malicious attackers [9].

C. Objectives of the Study

The primary focus of this study is to create a secure framework for user authentication in web applications using Visual Cryptography. Specifically, this study aims to:

1) Create a simple web application that requires a user to register an account or login into an existing account;
2) Implement a CAPTCHA generator;
3) Apply encryption techniques on the the resulting CAPTCHA image; and
4) Implement a visual cryptography scheme in the application's authentication system.

D. Research Questions

The following are the questions that the study aims to answer:

1) How effective is a visual cryptography scheme in preventing malicious attacks?
2) In what ways does implementing visual cryptography improve user authentication?
3) How feasible is the implementation of the framework in the creation of websites?

E. Significance of the Study

As more attackers exploit the vulnerability of unaware Filipinos, they will continue to dominate the country's cyberspace if no action is taken. Exposure to harms such as identity theft, credit card fraud, and forged payment systems leads to long term impacts to affected individuals. Individuals could lose money and intellectual property or could be impersonated to gain more data from close peers and family members [10]. Currently, there are only reactive solutions to protecting one's self from malicious attackers - one of which is reporting the incident to the Department of Information and Communications Technology (DICT) or the Department of Justice (DOJ) [11] which is not only time-consuming to report, but also extremely challenging to track down the attacker. According to Mankhair, et al. [12], one of the key characteristics of CAPTCHA is its preventative measures against optical character recognition (OCR) attacks and other related attack programs while still being readable by humans through common distortions. Thus, a proactive approach that places an additional burden to attackers is ideal to prevent the attack from happening in the first place.

II. Review of Literature

A. The Philippines' Exposure to Cybercrime

While the Internet was developed as one of the primary tools for the exchange of information and an accessible and efficient method of communication, it is inevitable that the online space would also be infiltrated by people with malicious intents. With this, it has urged the United Nations to set the standard of cybercrime protection by creating the Doha Declaration [13] to protect people online, just like in the physical world. Most countries followed suit, with the Philippines enacting Republic Act No. 10175 or "Cybercrime Prevention Act of 2012" [14] to address illegal actions committed in the digital space. However, cybercrime persisted and has still emerged as the fastest rising economic crime according to a report from the country's National Security Policy (NSP) 2017 to 2022 [15]. Many criminals have taken advantage of the accessibility, efficiency, and anonymity when they commit crimes on the Internet.

The rise of the digital space in the Philippines. As of January 2021, 98.5% of the Philippine population aged 16 to 64 own a smartphone and 77.3% own a laptop or desktop computer, two of the primary devices used to access the Internet. The country's users have amassed an average of 10 hours and 56 minutes of usage per day on all devices, with 4 hours and 15 minutes of the time dedicated to social media platforms [1]. In the preliminary results of a Philippines-based survey called the "2017 Survey on Information and Communication Technology (SICT) for the Information Economy (IE)", it reported that almost all of the establishments in the ICT industry used Internet-dependent communication equipment and methods for their businesses, with 97.2% having internet access. Most of these businesses use the Internet extensively for handling their business, downloading and requesting forms, or for maintaining their respective establishment's website [16]. Given the number of citizens who are exposed to or use these ICT-related products and services, if these establishments are affected by malicious attacks, all of their users would consequently be affected as well. This demonstrates how entrenched social media use is in the daily habits of Filipinos, resulting in a more vulnerable population.

The prevalence of cyber attacks in the Philippines. According to the United States International Trade Administration [17] , the Philippines has been ranked the 5th country in the world to be most likely attacked in the digital space in 2019 and in 2016, a detrimental data breach on the Commission on Elections compromised 70 million votes that were registered, making it one of the biggest data breaches the country has ever experienced. Based on the 2020 Full Global Cyber-Safety Index from SEON Technologies [18], a company that focuses on cybercrime and fraud prevention, the Philippines ranks 70th out of 94 with a 4.9 rating out of 10 in the total cyber-safety score. This means that the country is one of the most affected and at risk countries for different types of cybercrimes. A study conducted by TransUnion [19] during the coronavirus disease 2019 (COVID-19) pandemic observed that 44% of Philippines-based consumers have fallen into the trap of digital fraud at the beginning of 2021, where 48% of the targeted citizens were of age ranging from 19 to 26 years old and 42% ranging from 27 to 41 years old. In the same study, it discovered that there has been a 31% increase in digital fraud attempts against enterprises, especially in the telecommunications, logistics, and financial industries. In the 2021 webinar conducted by Secuna, the first and only cybersecurity testing company in the Philippines, many cybersecurity advocates and specialists urge both the government and private companies to craft more stringent, protective, and proactive policies as the Philippines continues to be the 4th ASEAN country most likely to be attacked by ransomware and the 82nd cybersecurity-ready country [20]. This exposes the massive vulnerability that citizens, organizations, and institutions ought to avoid in the years to come.

The perception of Internet security in the Philippines. It is also important to note that the cause of the problem not only exists in the technical aspect. There is currently a lack of institutional information dissemination related to Internet security in the country, with the absence of proper courses in curriculums and with technical training sessions being too inaccessible and unaffordable for an average Filipino. A survey conducted by [2] does show promising results as majority of their study's respondents do practice online security measures. However, most of them do not understand the purpose for such practices. This further establishes that proper education and understanding is necessary for Filipinos to effectively protect themselves against attacks. According to the 2020 Unisys Security Index [21], a study conducted during the peak of the COVID-19 pandemic, when Filipinos were asked about their concerns on the four categories of security — namely national, financial, internet, and personal — internet security was typically deprioritized despite the transition to the online setup. The study proposes that there is a false sense of security among the people globally due to the emergence of the pandemic. This further demonstrates not only the lack of awareness from the people, but also the lack of willingness to learn and do their own research for protective measures. Over the years, the Philippines has been stricken with many massive cyber attacks, with individual citizens being the most vulnerable. These were due to failures in cyber regulation and security along with the unfamiliarity of the existence of the attacks. Evidently, there is a need for improvement and change.

B. The Use and Application of Visual Cryptography for Authentication

The use of visual cryptography in implementing security systems has been studied since the early 2010s. Albeit a specialization at its infancy, there have been multiple studies conducted on the implementation of visual cryptography schemes.

Visual cryptographic frameworks. Most frameworks that involve visual cryptography have the same process for the user. Specifically, the phases are divided into two parts - the login and registration phase. In the registration phase, the user creates an account by entering a username and a password. This password is concatenated with a randomly generated string and is translated to a CAPTCHA image. The image undergoes an encryption phase and outputs two shares - a user and server share, which are both needed to log into the website.

The encryption phase differs among the studies. Kumar, V. and Kumar, R. in 2015 [22] proposed the use of a simple (2,2) Visual Cryptography Scheme to divide the CAPTCHA image into a user and server share. The two shares are needed for decryption, and the final image only appears when both shares are present and stacked onto each other.

In 2014, Jose and Lakshmi [23] used three algorithms, starting with using the Blowfish algorithm, then the Splitting and Rotating algorithm, and then finally, the (2,2) Visual Cryptography Scheme. The sequence of the encryption process that Navarkar and Phalke [24] used in the same year is similar, but was instead called block transformation, rotation, and subpixel dividence. Both studies had a resulting output of two shares where one share is for the user and the other is for the server.

Studies from Sahare, et al. [25] and Chaudhari, et al. [26] used RGB pixel shuffling for the image cipher where values of the red, green, and blue components of the image is modified and manipulates in such a way that forms a new image that can be divided into the two shares.

Churi, et al. in 2017 [27] utilized three algorithms and techniques for the CAPTCHA image. First, the image undergoes a Balanced Block Replacement (BRR) method to convert the image into grayscale. Then, the Advanced Encryption Standard(AES) technique was applied. This technique is "a non-Feistel cipher that encrypts and decrypts 128-bits of block of data", according to Churi et al. Lastly, the Code Generation Technique using a simple calculation method was applied to generate the final text that will be displayed in the CAPTCHA, to be divided into two shares for the user and server.

III. Materials and Methods

The framework will simulate the authentication process of a web application. The user can register if they do not have an existing account and they can log in with their username and password if they have an existing account. In this framework, the user will be given an image — called a share — that they need to keep and it will serve as their password every time they need to login. The framework requires a visual cryptography scheme wherein an image with text, similar to a Completely Automated Public Turing Test To Tell Computers and Humans Apart or CAPTCHA, will be displayed for the user to read and input as their tool for authentication. It is modeled after the framework by Navarkar and Phalke [24] and Jose and Lakshmi [23]. The CAPTCHA image will only appear if the two images required for decryption are present.

1) Registration Phase: This is the initial phase that all users need to undergo to create their account. When a user registers for the website, they must create their desired username and key, commonly known as their password.This key will be concatenated with a randomly generated string from the server and the resulting string will be translated into a CAPTCHA image. The image will then be passed through multiple encryption phases and a (2,2) visual cryptography scheme which will result in two shares - the user and the server share. The first encrypted image, called the user share, is the half of the image that the user needs to keep. They can generate a new one if the initial one is compromised. The second encrypted image, called the server share, is stored in the web application's server and is the unique pair for the user's share. Having only one of the two shares will never allow any user to access an account.

2) Login Phase: This phase is for users with existing accounts. The user must enter their unique username and upload their share. Given their username, the server share is taken from the database. The user share will then be stacked with the server share and be decrypted to display the uniquely generated CAPTCHA image. The user must then type the displayed text in the image to successfully log into their account. If the CAPTCHA image does not display, then the user can detect whether the website is real or fake.

A. System Flowchart

The system flowchart, as shown in Figure 1 below, illustrates the process of the two phases in the framework. This flowchart is modelled after the studies conducted by Sahare, et al. [25], Jose and Lakshmi [23], and Churi, et al. [27] with a few additional tweaks.

B. Creating the Website

A web application will be created to simulate the authentication process shown in Figure 1. It will have a registration page and a login page. There will also be a simple page that displays the user's information once they are logged in, along with a simple logout button. The crucial aspect of the website is the authentication, hence, this study will primarily focus on these essential pages.

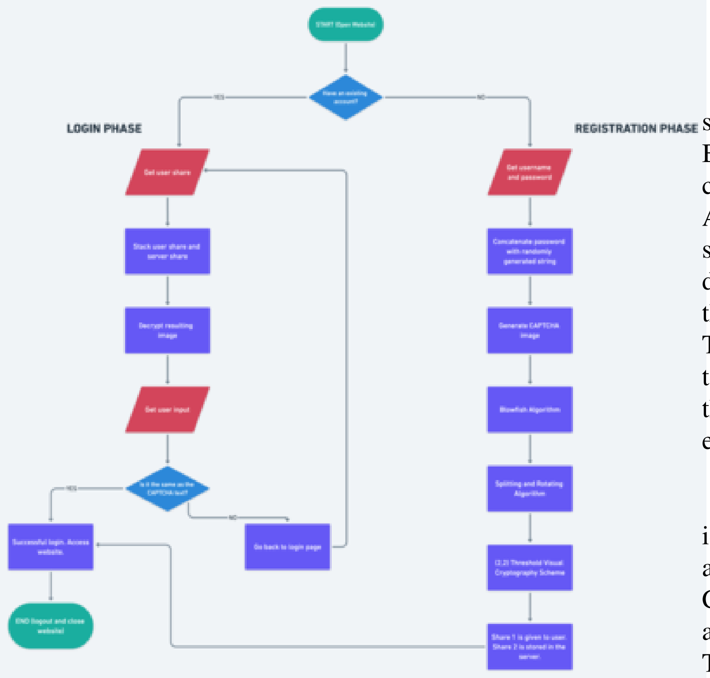
START (Open Website)
Have an existing account?
YES
NO
LOGIN PHASE
REGISTRATION PHASE
Get user share
Stack user share and server share
Decrypt resulting image
Get user input
Is it the same as the CAPTCHA text?
YES
NO
Successful login. Access website.
Go back to login page
END (logout and close website)
Get username and password
Concatenate password with randomly generated string
Generate CAPTCHA image
Blowfish Algorithm
Splitting and Rotating Algorithm
(2,2) Threshold Visual Cryptography Scheme
Share 1 is given to user. Share 2 is stored in the server.

Fig. 1. Web Application System Flowchart

C. CAPTCHA Image Generator

The system will have a function that generates its own CAPTCHA image for the user. This image will only be generated after the concatenation of the user's key and the server's randomly generated string. The image will only contain monochromatic colors (black and white) for its pixels. This is because it is the simplest to implement, as the colors could be easily associated with the binary elements 1 and 0, while still achieving the desired effect for its security.

D. Encryption Phase

Two encryption methods will be used in this study, modeled after the studies conducted by Navarkar and Phalke [24] and Jose and Lakshmi [23].

1) Blowfish Algorithm: This algorithm was designed by Bruce Schneier in 1993 to be "a fast, free alternative to existing encryption algorithms" [28]. The algorithm is a symmetric block encryption algorithm and has been used in email encryption and password management tools [29]. According to Desai et al. [30], the following can be observed:

1) The algorithm is fast — it encrypts data on large 32-bit microprocessors at a rate of 26 clock cycles per byte
2) The algorithm is compact — it can run in less than 5K of memory
3) The algorithm is simple — it uses addition, XOR, lookup table with 32-bit operands
4) The algorithm is secure — the key length is variable, it can be in the range of 32 448 bits: default 128 bits key length
5) The algorithm is suitable for applications where the key does not change often, like communication link or an automatic file encrypter.
6) The algorithm is unpatented and royalty-free.

This will be used because of its multiple advantages in speed and security. Singh and Maini [31] observed that the Blowfish algorithm performed better when compared with commonly used encryption algorithms (DES, 3DES, and AES). The Blowfish algorithm does not have any known security weak points as of now. Even AES performed poorly due to its requirement of more processing power. Thus, the Blowfish algorithm is an ideal encryption technique. This is reiterated by Singh et al. [32], observing that in terms of encryption time, decryption time, and throughput, the Blowfish algorithm always performs better than other encryption algorithms.

2) Splitting and Rotating Algorithm: This method, as studied by Ince et al. [33], is "developed for differing human users and computer programs from each other by mainly splitting CAPTCHA image into several parts with rotation and drawing a great deal of lines and circles randomly to the background". The algorithm will be applied to the CAPTCHA image to protect it against Optical Character Recognition (OCR) programs . Given that attackers also have access to multiple technological advancements such as OCR systems, this algorithm provides an additional layer of difficulty for such attacks because the rotation of the alphanumeric characters provides confusion in recognizing the exact one [33].

E. (2,2) Visual Cryptography Scheme

This visual cryptography scheme was created by Moni Naor and Adi Shamir in 1994 and is the simplest. The detailed process of the scheme in this study emulates some of the methods used by Verma and Khemchandani [34] and Berry [35]. It splits a secret message — text displayed in an image — into two carefully divided components. The CAPTCHA image has P pixels, which will be encrypted into two subpixels called shares. To obtain the two shares, each pixel will be divided into 4 quadrants, as shown in Figure 2.

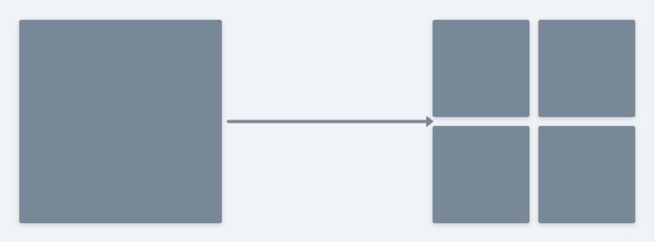

Fig. 2. Visualization of a pixel divided into 4 quadrants

These 4 quadrants will be shaded according to the original CAPTCHA image. The shading is distributed in such a way that having only one of the shares would not reveal the original image. If a P pixel is black, the 4 quadrants will all be shaded black. To get the 2 shares, the program will randomly choose any of the 3 possible permutations shown in Figure 3, modelled after the study conducted by Melgar and Farias [36].

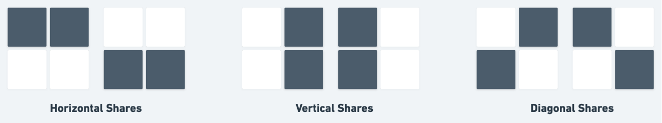

Fig. 3. Possible shading of pixels for the two shares to simulate a black pixel

The user share will take one of the halves of the permutation and the server share will take the other one. Conversely, if the P pixel is white, there would only be two shaded pixels instead of all 4, which means that there are 6 permutations for the shading. The other indicator for a white pixel is to use the same shading pattern for both the user share and the server share. Similarly, the shade is randomly chosen as well. Once this distribution has been executed for all P pixels, it would result in the 2 needed shares for the program to work.

There is no need to use all 3 permutations. The encryption would still work and be secure even if only the horizontal share was used for all pixels, but using all 3 permutations gives the CAPTCHA image more variety in its resulting image.

F. Decryption Phase

Decryption only occurs if and only if the user share is the correct pair for the server share, given the unique username. Otherwise, the resulting CAPTCHA image will be garbled and simply be random black and white pixels. If the two needed shares are correct, the counterparts of the algorithms stated in the encryption phase will be used again to decrypt the image. Then, decrypting the CAPTCHA image after stacking requires the human visual system (HVS). This is done by reading the resulting text that is displayed on the image and typing it onto the text box provided. After correctly entering the text, the user is then logged in and is able to access the functionalities of the website.

REFERENCES

[1] DataReportal, “Digital in the philippines: All the statistics you need in 2021 - datareportal – global digital insights,” Nov 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-philippines

[2] C. Omorog and R. Medina, “Internet security awareness of filipinos: A survey paper,” *International Journal of Computing Sciences Research*, vol. 1, no. 4, p. 14–26, 2018.

[3] A. M. Qadir and N. Varol, “A review paper on cryptography,” *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019.

[4] ElProCus, “Cryptography : Different types, tools and its applications,” Jan 2020. [Online]. Available: https://www.elprocus.com/cryptography-and-its-concepts/

[5] A. Vinodhini and L. Anbarasi, “Visual cryptography for authentication using captcha,” *International Journal of Computer and Internet Security*, vol. 2, no. 1, p. 67–76, 2010.

[6] J. Devanesan, “Phishing scams dominate the philippines cybercrime landscape,” Aug 2020. [Online]. Available: https://techwireasia.com/2020/08/phishing-scams-dominate-the-philippines-cybercrime-landscape/

[7] E. V. Abadilla, “Kaspersky: Password theft on the rise in ph, sea,” May 2021. [Online]. Available: https://mb.com.ph/2021/05/25/kaspersky-password-theft-on-the-rise-in-ph-sea/.

[8] “Fico survey: Banking passwords are problematic! filipinos want biometrics,” Jul 2020. [Online]. Available: https://www.fico.com/en/newsroom/fico-survey-banking-passwords-are-problematic-filipinos-want-biometrics

[9] S. Nisha and A. N. Madheswari, “Prevention of phishing attacks in voting system using visual cryptography,” *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, vol. 1, no. 4, p. 14–26, 2016.

[10] Kaspersky, “What is phishing and how does it affect email users,” Jan 2021. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/what-is-phishings-impact-on-email

[11] D. of Justics, “Reporting of cybercrime incidents.” [Online]. Available: https://www.doj.gov.ph/reporting_cybercrime.html

[12] S. Mankhair, A. Raut, M. Mohimkar, K. Sukal, and A. Khedekar, “Secured captcha password verification using visual cryptography,” *International Journal of Engineering Science and Computing*, vol. 6, no. 5, p. 5428–5251, 2016.

[13] United Nations, 2015.

[14] 2015.

[15] C. Castillo, “Defending the philippines’ cyberspace amid covid-19.” [Online]. Available: http://www.ndcp.edu.ph/index.php/defending-the-philippines-cyberspace-amid-covid-19/

[16] P. S. Authority, “2017 survey on information and communication technology (sict) - for information economy (core ict industries): Preliminary results,” Feb 2020. [Online]. Available: https://psa.gov.ph/surveys/sict

[17] I. T. Administration, “Philippine cybersecurity,” Apr 2020. [Online]. Available: https://www.trade.gov/market-intelligence/philippine-cybersecurity

[18] G. Varga, “Global cybercrime report: Which countries are most at risk? 2022,” Dec 2021. [Online]. Available: https://seon.io/resources/global-cybercrime-report

[19] T. Philippines, “One year after covid-19 pandemic declared, new transunion research shows digital fraud attempts from the philippines have increased,” Mar 2021. [Online]. Available: https://newsroom.transunion.ph/one-year-after-covid-19-pandemic-declared-new-transunion-research-shows-digital-fraud-attempts-from-the-philippines-have-increased

[20] M. B. Technews, "Ph in the top list of cyber-attacks in asean," Sep 2021. [Online]. Available: https://mb.com.ph/2021/09/10/ph-in-the-top-list-of-cyber-attacks-in-asean/

[21] Unisys, "2020 unisys security index: Philippines," Jul 2021. [Online]. Available: https://www.unisys.com/es/unisys-security-index-2020/philippines/

[22] V. Kumar and R. Kumar, "Detection of phishing attack using visual cryptography in ad hoc network," *2015 International Conference on Communications and Signal Processing (ICCSP)*, 2015.

[23] A. Jose and S. Lakshmi, "Web security using visual cryptography against phishing," *Middle-East Journal of Scientific Research*, vol. 20, no. 12, p. 2626–2632, 2014.

[24] A. Navarkar and D. Phalke, "Anti phishing using visual cryptography," *International Journal of Science and Research*, vol. 3, no. 2, p. 305–310, 2014.

[25] V. Sahare, S. Jain, and M. Giri, "Anti-phishing system using visual cryptography," *International Journal of Emerging Technologies in Engineering Research*, vol. 3, no. 3, p. 30–37, 2015.

[26] M. Chaudhari, N. Chaudhari, S. Kanade, S. Bhadre, and D. Bhagat, "Phishing attack prevention using visual cryptography," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 8, no. 4, p. 168–173, 2019.

[27] T. Churi, P. Sawardekar, A. Pardeshi, and P. Vartak, "A secured methodology for anti-phishing," *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2017.

[28] B. Schneier, "The blowfish encryption algorithm." [Online]. Available: https://www.schneier.com/academic/blowfish/#

[29] M. Gibbs, "Blowfish encryption: Strength & example." [Online]. Available: https://study.com/academy/lesson/blowfish-encryption-strength-example.html

[30] S. Desai, C. Mudholkar, R. Khade, and P. Chilwant, "Image encryption and decryption using blowfish algorithm," *International Journal of Electrical and Electronics Engineers*, vol. 7, no. 1, p. 243–248, 2015.

[31] S. Singh and R. Maini, "Comparison of data encryption algorithms," *International Journal of Computer Science and Communication*, vol. 2, no. 1, p. 125–127, 2011.

[32] G. Singh, A. K. Singla, and K. S. Sandha, "Superiority of blowfish algorithm in wireless networks," *International Journal of Computer Applications*, vol. 44, no. 11, p. 23–26, 2012.

[33] I. F. Ince, I. Yengin, Y. B. Salman, H.-G. Cho, and T.-C. Yang, "Designing captcha algorithm: Splitting and rotating the images against ocrs," *2008 Third International Conference on Convergence and Hybrid Information Technology*, vol. 2, 2008.

[34] J. Verma and V. Khemchandani, "A visual cryptographic technique to secure image shares," *International Journal of Engineering Research and Applications*, vol. 2, no. 1, p. 1121–1125, 2012.

[35] N. Berry, "Visual cryptography." [Online]. Available: https://datagenetics.com/blog/november32013/index.html

[36] M. E. V. Melgar and M. C. Farias, "A (2,2) xor-based visual cryptography scheme without pixel expansion," *Journal of Visual Communication and Image Representation*, vol. 63, 2019.

Louise Gabrielle L. Talip Loys is a senior BS Computer Science student studying at the University of the Philippines Los Baños. She is a member of the Alliance of Computer Science Students UPLB and the university's official debate organization, the Parliament: UPLB Debate Society. Her adviser is Prof. Joseph Anthony C. Hermocilla and she is a member of the Systems Research Group. She has constantly been a part of the Top 50 CAS Students and she was awarded as the CAS Outstanding Student in the Sciences in 2021. Her research interests include cybersecurity, web development, artificial intelligence, and data science.