Combination of Alphanumeric Password and Graphic Authentication for Cyber Security

Joseph Teguh Santoso[1*], Budi Raharjo[2] and Agus Wibowo[3]

[1*] Rector, Faculty of Computer and Business University of Computer Science and Technology (STEKOM University) Semarang Indonesia. joseph_teguh@stekom.ac.id, Orcid: https://orcid.org/0000-0001-6227-1111

[2] Lecturer, Faculty of Computer and Business University of Computer Science and Technology (STEKOM University) Semarang Indonesia. budiraharjo@stekom.ac.id, Orcid: https://orcid.org/0000-0001-6192-0888

[3] Associate Professor, Affiliati Faculty of Computer and Business University of Computer Science and Technology (STEKOM University) Semarang Indonesia. agus.wibowo@stekom.ac.id, Orcid: https://orcid.org/0000-0002-1251-0468

Received: August 29, 2023; Accepted: November 22, 2023; Published: February 28, 2024

Abstract

The main objective of this research is to create a more secure and user-friendly password-generation method that is less vulnerable to attacks such as shoulder surfing. Similarly, while textual or alphanumeric passwords are not entirely secure, they also come with certain limitations, including issues related to memory. The novelty of this research is the development of a new algorithm (Secure Password Algorithm/SPA) for password generation that uses graphics to generate textual input from users based on user perceptions. This method is more resilient against attacks like shoulder surfing and offers a more secure and user-friendly way of creating passwords. This research uses a combination of literature review and SPA proposals to create passwords with graphical and encryption techniques. The literature review examines the weaknesses of existing graphical and text password methods. The proposed algorithm focuses on user perception and confidential data to create more secure and easy-to-use passwords. The research results show that this research can provide a new, more secure, and user-friendly method of generating passwords such as shoulder surfing. Research supports software implementation of these algorithms and psychometric, psychological, and psychiatric studies to improve user input and protect systems from malicious attacks. Graphical passwords provide better recall compared to textual passwords, and the proposed algorithm for password generation using graphical and encryption techniques provides a more secure and user-friendly method of password generation that is less vulnerable to attacks such as shoulder surfing. The proposed new encryption algorithm has succeeded in overcoming various potential weaknesses and attacks on previous encryption methods. The test results demonstrate the efficiency and near invulnerability of the SPA algorithm against brute force attacks on specific security parameters. Tested alongside AES, shows comparable security levels, particularly in resource-constrained environments. To address doubts, the paper establishes evaluation standards for computational complexity, resistance to known attacks, and adaptability to evolving threats. The

Journal of Interner Services and Information Security (JISIS), volume: 14, number: 1 (February), pp. 16-36
DOI: *10.58346/JISIS.2024.I1.002*

*Corresponding author: Rector, Faculty of Computer and Business University of Computer Science and Technology (STEKOM University) Semarang Indonesia.

algorithm has the potential to be a stronger and more secure solution for generating passwords to safeguard confidential user information.

Keywords: Password Generation, Encryption Techniques, Authentication.

1 Introduction

Authentication involves the process of verifying whether an individual is an authorized user with permission to access specific services or resources. Besides alphanumeric passwords, other methods like smart cards and biometrics are also employed (Cockell & Halak, 2020; Rui & Yan, 2019). Nevertheless, despite these alternatives, alphanumeric passwords still dominate and are likely to continue doing so due to smart cards requiring PIN and biometrics being associated with privacy concerns (Brostoff & Sasse, 2000; Dee et al., 2022; Jayapal, 2017). Alphanumeric passwords are more susceptible to risks compared to graphical passwords since users often opt for shorter passwords for ease of memory, making them vulnerable to easy attacks. In addition, text or alphanumeric passwords are vulnerable to attacks by dictionaries, key recorders, password guessing, over-the-shoulder viewing, spying software, etc (Nyirongo et al., 2017). Typically, individuals prefer to create passwords that are short and easy to recall rather than opting for complex ones. This inclination arises from the fact that while text passwords offer a certain level of strength against guessing, they are also challenging to memorize (Nyirongo et al., 2017). However, there are always questions involving generating text passwords which often have answers that are quite difficult for users to remember when creating them. The widely employed computer authentication technique involves utilizing an alphanumeric password, yet this approach possesses inherent weaknesses that malicious actors can exploit to undermine security (Nyirongo et al., 2017). In alphanumeric passwords, algorithm development is required because strong passwords require strong user memory as well. Gokhale & Waghmare, (2014) stated that many images are easier to remember, so graphic passwords are safer than alphanumeric passwords. However, graphic passwords have a weakness, namely "shoulder surfing attack" (Nyirongo et al., 2017). Numerous researchers contend that graphical passwords necessitate further investigation to address the vulnerability of over-the-shoulder attacks (OSA), while simultaneously navigating the trade-off between security and usability (Buriro et al., 2021; Zhou et al., 2019). Thus, this study proposes a novel approach, known as SPA, aiming to produce highly resilient passwords that are exceptionally challenging for modern computers and even supercomputers to crack. SPA centers around the crucial aspect of password strength and emphasizes the use of Whirlpool Encryption (WE) in the design and development process to generate exceptionally robust passwords, all while considering the user's memory capabilities.

2 Literature Review and Hypothesis Development

Authentication Methods based on Graphics or Visual Elements

Graphic passwords offer improved memorability compared to complex alphanumeric passwords (Islam et al., 2023). As a result, many researchers have explored the concept of picture passwords (Gokhale & Waghmare, 2014; Sreelatha et al., 2011; Zhou et al., 2019). However, image-based passwords are susceptible to OSA (Rui & Yan, 2019; Zhou et al., 2019), rendering them vulnerable. In contrast, alphanumeric passwords provide higher security compared to picture passwords. However, as the number of characters increases, they become more difficult to remember. To address OSA for picture passwords, alternative approaches have been proposed, including grouping, relocating, disguising, cued recall, and line recall, but their efficiency remains limited (Ho et al., 2021). The grouping technique aims to divert the attacker's attention by presenting additional images, while the move to another location

method involves shifting the password point from one position to another. However, neither of these alternatives effectively safeguards against OSA (shoulder surfing attack). Bianchi et al. introduced this scheme to relocate the target instead of solely clicking on it (Zhou et al., 2019). Furthermore, the disguising technique is a technique for searching and selecting passwords from the first image, second, and third targets, this means the chronological order of the images followed. Nevertheless, this approach fails to offer enhanced security. In this method, users are required to locate the target, mentally eliminate the portion of the image without the target, and then click on the remaining result in a different location. “The effectiveness of this technique hinges on the user's capability to discern the correct targets amid these distractors” (Tippannavar et al., 2023).

The Cued Recall method instructs users to recall a particular location and target it. Its purpose is to alleviate the memory burden on individuals. This system is referred to as the Loci metric (Wang et al., 2023). According to Kenneth & Olujuwon, (2021), Users, upon focusing on an image initially, may remember certain parts of the image to use as a password. If an attacker can determine the image's position on the screen, they might only require a mouse watchdog to capture click-based graphical passwords. Alternatively, if the attacker can identify when the user clicked the mouse button (and some users may not stop moving the cursor while clicking), a screen scan might be enough to locate the image and be sufficient to capture click-based graphical passwords. OSA can also reveal the user's password in one login since the entire password is visible on the screen when the user enters it” (Nam et al., 2020). Next is the method of draw-metric (Deane & Henderson, 1995), this method requires the user to recall and recreate intricate images from memory. This recall is done without the aid of memory or cues so recall becomes difficult (Craik et al., 1987).

DAS (Jermyn et al., 1999), is the pioneering memory-based drawing authentication system. Users must create their password designs on a two-dimensional grid using either a continuous pen line or multiple pen lines that originate from various cells on the grid. While the user can opt for complex scribble drawings, this technique is limited to small grids and remains susceptible to OSA. On the other hand, BDAS (Background DAS), proposed by Dunphy (Nguyen & Zeng, 2011), is an extension of the DAS technique. It incorporates a background image to create more challenging passwords. The concept involves providing memory cues through an image grid and a background image. The careful selection of images depends on the available potential locations (Jiang et al., 2021). Lastly, the Ink Authentication Technique is a less apparent graphical authentication method that relies on clues derived from blurred images. Users are shown an inkblot to memorize and are asked to recall the first and last letters of the word representing the inkblot. The inkblot locations will also change from one to another, and the user usually remembers the correct inkblot instructions.

Encryption Techniques

Encryption technique is a process for securing information by changing the original text or data into a form that cannot be understood (ciphertext) using a certain algorithm. Only the recipient who has the secret key or decryption method can return the data to its original form (plaintext). The main purpose of encryption is to guarantee the privacy, integrity, and authentication of data, and to protect information from access by unauthorized parties.

Shift Chipper Technique

In this approach, each letter and character undergo a fixed number of shifts (referred to as "shift"). All elements are then shifted accordingly based on this fixed number, and the final character wraps back to the beginning. If the text of METHOD and shift 1, the letter "M" will be replaced by "N", the letter "E"

will be replaced by "F", the letter "T" will be replaced by "U", the letter "H" will be replaced by "I", the letter "O" will be replaced by "P" and the letter "D" will be replaced by "E". For the same word METHOD, sliding 27 or 53 will produce the same result. However, this technique has a weakness, namely this encryption technique is quite weak. It only requires permutations and combinations of twenty-six characters, and the cipher text can be directly decrypted without knowing the shift number.

Affine Cipher Technique

In this method, the requirement is that α and β should have a greatest common factor equal to one. Similar to the shift cipher technique, where the last character is connected to the first character, this encryption also relies on permutations and combinations of 26 characters. For instance, in the text “FINE” “F” will be encrypted as “V”, “I" becomes "W," “N” becomes “P”, and “E” becomes “W”. Thus, “FINE” will be encrypted to “VWPM” using the affinity cipher. However, this technique has a significant drawback as it is quite vulnerable. With only 26 characters (β) and twelve possible alternatives for α, where the greatest common factor of twenty-six characters is 1, the total key choices amount to 26x12=312.

Vigenere Cipher Technique

In this technique, the strength of security relies on the length and randomness of the password (Grammatopoulos, A.V., 2022). The cryptosystem involves selecting a keyword and assigning numbers from 1 to 26 to each character. These numbers are then used as shifts to encrypt each character of the plaintext (this is commonly referred to as a vector). For example, if the word "TOGETHER" is changed to a number with the alphabetical rules numbering 26 then if encrypted the key shift will be 19, 14, 6, 4, 19, 7, 4, 17, Each character will be subjected to the corresponding shift according to the assigned vectors. However, this technique has a drawback as it lacks security and is susceptible to various attack methods, including known plaintext attacks, selected ciphertext attacks, and cryptanalysis attacks.

Substitution Cipher Technique

In this encryption scheme, every letter is substituted with another letter, occasionally leaving some letters unchanged to enhance complexity. This approach renders frequency analysis susceptible to exposing the ciphertext and decrypting the plaintext. Frequency analysis poses a threat to deciphering the original text. In this particular text cipher technique, all letter characters are replaced with randomly chosen characters from the alphabet.

Block Chipper Technique

Among the methods mentioned above, cryptanalysis stands out as a successful attack approach due to specific cipher characters originating from a particular plaintext, enabling the decryption of not only those characters but also others through careful analysis. To counteract cryptanalysis, block ciphers were designed in a manner were altering one character affects the entire block, thereby significantly raising the difficulty level for decrypting text using cryptanalysis.

3 Cryptosystems

Des Cryptosystem

DES (Data Encryption Standard) (1973) is a symmetric key cryptosystem. Initially, this was introduced with a key length of 56 bits, which was deemed secure enough at that time until computational power became insufficient to defend against successful brute-force attacks. However, as computing power

advanced over time, DES became susceptible and eventually outdated. It employs a block size of 64 bits, where data blocks are divided into two parts, following the Feistel Circuit structure. In terms of security, DES proved inadequate due to its relatively slow speed. The encryption process in this cryptosystem handles blocks independently. In DES, input messages are processed as L_0 R_0, with each message consisting of 12 bits ($L_{(0)}$ and $R_{(0)}$ having 6 bits each). In each loop, the $_i$-th round generates outputs L_i and R_i based on the inputs $L_{(i+1)}$ and $R_{(i-1)}$. This process continues for all rounds, as depicted in Figure 1. From Figure 1, $L_{(i-1)}$ is utilized as input to produce $R_{(i)}$, while $L_{(i)}$ is used to derive $L_{(i+1)}$. Consequently, every character is interconnected, and modifying one character affects the entire character block. The weakness of the DES Cryptosystem is Brute Force Attack and gradually the DES cryptosystem became unusable.

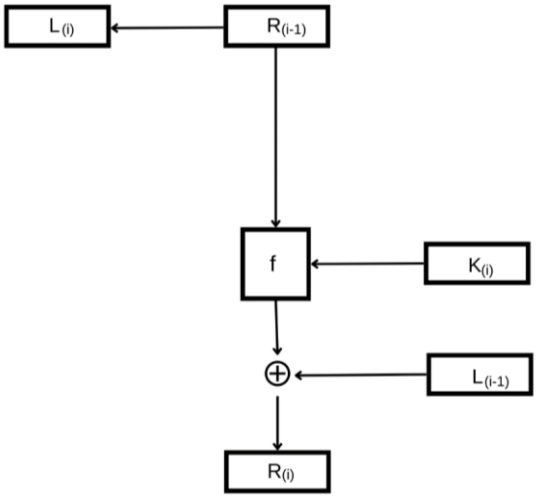


Figure 1: DES Block Diagram (Source: Author Elaboration)

AES Cryptosystem

In AES, all data blocks are considered as a single matrix. In terms of AES encryption speed, it is considered faster than DES because it is entrenched in the principle of substitution and permutation. The algorithm also has to operate with 128 bits of input, Simultaneously, the system should be capable of seamlessly integrating with a wide variety of hardware devices. AES comprises four layers. The varied key sizes in AES pose a challenge to hardware compatibility. AES cryptosystem involves multiple steps, starting with the Byte Substitution Transformation (BS) that safeguards the system from differential and linear cryptanalytic attacks. During this phase, each byte undergoes conversion using “the S box”, a matrix that transforms characters into specific values for the subsequent round.

Next, the Shift Row Transform (SR) is implemented to disperse bits across numerous rounds. This process entails circularly rotating all rows within the matrix. The results obtained from the initial layer undergo left shifts with different offsets to form the matrix. Subsequently, the Mix Column (MC) Transformation works in conjunction with layer 2 to complete the process. During this phase, matrix values from the shift row transformation are blended into specific columns, chosen based on specific criteria, and not rigidly fixed each time. The values received from layer 2 undergo multiplication by a binary matrix that can be adjusted as per the algorithmic requirements, allowing for easy adaptability for SPA protection. This mix column transformation significantly bolsters the encryption's strength. In the last stage, the ARK layer applies an XOR operation between the round key and values from the mix column transformation layer. This specific round involves XORing the bytes received from round 3 with

the key, to minimize vulnerability to linear attacks (LnA) that could potentially compromise encryption. Despite its strengths, AES encryption has been compromised faster by researchers using sophisticated computing power, making it less secure (Yaseen Khudhur et al., 2018). Additionally, its compatibility with hardware is affected by four different key length versions, and it tends to be relatively slow.

RSA Algorithm

This is a cryptographic system based on “public key encryption”, that allows the public access to the key used for encryption, while the decryption key remains restricted to authorized users. The concept of public key encryption emerged after symmetric key encryption faced challenges. Diffie-Hellman was the first to publicly introduce the idea of cryptosystems with public keys (Sharma & Mittal, 2021). To use the RSA Algorithm, the recipient of the encrypted message selects 2 large main numbers, "p" and "q," and multiplies them to obtain the value "n." The encryption exponent "e" is chosen so that the greatest common divisor of "e," (p-1), and (q-1) is 1. The pair (n, e) is sent to the sender of the plaintext message. The sender then writes the message "m," calculates "c," and sends the result C = me (mod n) back to the original recipient as an encrypted message. The recipient, knowing "p" and "q," can find the decryption exponent "d" ≡ 1 (mod ((p-1) (q-1))) and use the equation m ≡ cd (mod n) to decrypt the message "m." Despite its effectiveness, the RSA Algorithm has three vulnerabilities. The first vulnerability is the Coppersmith attack, where knowledge of the first or last quarter of "n" along with "p" allows for efficient factorization and message decryption. The Bone attack, another vulnerability, exploits knowledge of the last digits of "d" and "m" to find "d" with linear time efficiency in base 2. Lastly, “the Weiner attack targets cases where the exponent "e" is not sufficiently large, making it possible to break the RSA algorithm” (Blömer & May, 2004).

Hash Function (HF)

This has a central role in various cryptographic algorithms. These functions take input messages of arbitrary length and produce fixed-length output messages. They are classified as one-way functions, satisfying three key conditions. Firstly, they must calculate the hash result “h(m)” for any message "m" quickly. Secondly, it should be practically impossible to discover an alternative message "m'" where the hash of "m'" matches a specific given hash value "y”. Lastly, It should be extremely difficult, computationally speaking, to find two distinct messages, message1, and message2, that result in the same hash value (h(message1) = h(message2)), ensuring resistance to strong collisions. Due to this property, HF is often referred to as a collision-free function, making it extremely difficult to find two distinct messages (m1 and m2) with the same hash value (h(m1) = h(m2)).

Efficiency HF

The HF generates the Hash value for each element within a data set. These functions involve rapid mathematical operations and exhibit deterministic and consistent behavior. When hashing data, the Hash Function utilizes its algorithm to distribute the data effectively, and this algorithm significantly impacts its efficiency. Depending on specific requirements, the Hash Function algorithm is specially designed to enhance efficiency and protect against potential attacks.

Disadvantages of Hash Functions

Hash Functions are susceptible to infinite collisions, which occur when different inputs produce the same output, owing to their capacity to take arbitrary-length inputs and produce fixed-range outputs. A potential compromise of Hash Functions involves finding a pair of input strings that yield the same Hash

output, known as a “Hash Collision”. There are different types of collision attacks on Hash Functions. The Pre-Drawing Attack involves determining and calibrating the Hash value based on certain input, setting, or calibrating it with plain text. On the other hand, the Birthday Attack delves into probability theory and random groups, seeking pairs with the same Hash value, presenting a 50% chance of breaking crash resistance.

Whirlpool Cryptosystem

This Hash function relies on a compression function that operates on two inputs: the chaining variable (obtained from the previous step) and a block of "b" bits, producing an output of size n bits. The final chaining variable represents the Hash value.

The Frame of HASH Whirlpool

In this encryption technique, the message is segmented into a series of blocks m1, m2, m3, ..., mt. The Hash function utilized in this encryption can be illustrated as presented in Figure 2. H_0 represents the initial value, “$H_i = E(H_{i-1}, m_i) \oplus H_{i-1} \oplus m_i$” stands for the intermediate value, and Ht denotes the final Hash Code value.

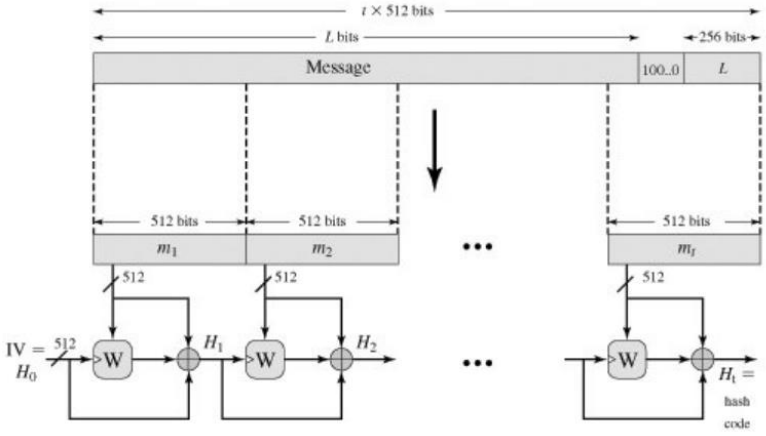


Figure 2: Message Summary Generation using WE (Pachghare, 2019; Tao & Wu, 2015)

Algorithm Task (Whirlpool)

This structure performs four essential tasks: firstly, it adds bit padding; next, it satisfies the length requirement; thirdly, it employs a Hash matrix; and finally, it processes the message into W blocks. These carefully designed steps aim to address all the successful attacks Over time, various encryption methods have been introduced, and these have been implemented in the past. In assignment 1, additional 0 bits are appended to the message to ensure it becomes an odd multiple of 256. If the message already has an even multiple of 256, it is concatenated with 256 bytes of value 0 to achieve an odd multiple of 256. However, if the message has an odd number of 256 bits, it is filled with 512 bits, resulting in the number of padding bits ranging from 1 to 512 bits. These extra bits consist of one "1" bit followed by the remaining "0" bits. In assignment 2, which deals with the length requirement, 256 bits are added to the message. As a result of the first two tasks, the integer length becomes a multiple of 512 bits. In the third task, a Hash matrix of size 8 x 8 is introduced, where all the bits are set to "0". Finally, during the 4^{th} task, the message undergoes processing into 512-bit blocks, which are subsequently utilized as input for the W block.

Block W Ciphers

The main reason behind the increased threats of WE compared to other encryption algorithms in the MD family (AES), is the W Block cipher. With a 512-bit block size, the W cipher offers enhanced security compared to the smaller key sizes of 128, 192, and 256 used in AES. Additionally, the fixed key size of 512 bits makes implementation straightforward and ensures better compatibility with various hardware types. Since WE use a fixed number of rounds (10 rounds), its implementation is easier compared to AES, which offers multiple round options, limiting its hardware compatibility. WE operate with an 8 X 8-byte state representation, and the more distinct the state representation, the slower the diffusion, requiring more rounds for the cipher. Although the developers of Whirlpool could have designed Rijndael to work with a 4 X 16-byte state for a 512-bit block length, it would have necessitated numerous rounds and resulted in significantly slower performance (Pachghare, 2019; Tao & Wu, 2015).

	W	AES
Block size (bits)	512	128
Key size (bits)	512	128, 192, or 256
Matrix orientation	Input is mapped row-wise	Input is mapped column-wise
Number of rounds	10	10, 12, or 14
Key expansion	W round function	Dedicated expansion algorithm
GF(2^8) polynomial	$x^8 + x^4 + x^3 + x^2 + 1$ (011D)	$x^8 + x^4 + x^3 + x + 1$ (011B)
Origin of S-box	Recursive structure	Multiplicative inverse in GF(2^8) plus affine transformation
Origin of round constants	Successive entries of the S-box	Elements 2^i of GF(2^8)
Diffusion layer	Right multiplication by 8 x 8 circulant MDS matrix (1, 1, 4, 1, 8, 5, 2, 9) - mix rows	Left multiplication by 4 x 4 circulant MDS matrix (2, 3, 1, 1) - mix columns
Permutation	Shift columns	Shift rows

Figure 3: Comparison of Block W on WE and AES (Pachghare, 2019)

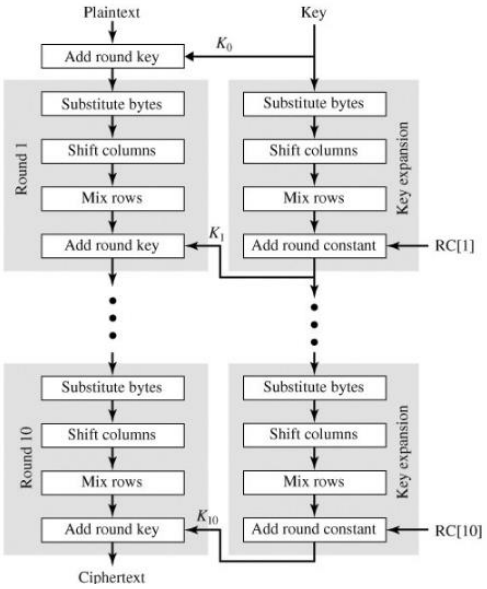


Figure 4: W Block of WE (Pachghare, 2019) Page 363

Whirlpool employs four distinct transformations, (AK, Byte Substitution (SB), Shifting of Column (SC), and Mixed Row (MR). The variable "r" depends on the function RF and the rotation W(K), and “Kr” represents the rotation key matrix for the corresponding rotation "r". The main input for the entire algorithm is denoted by "K".

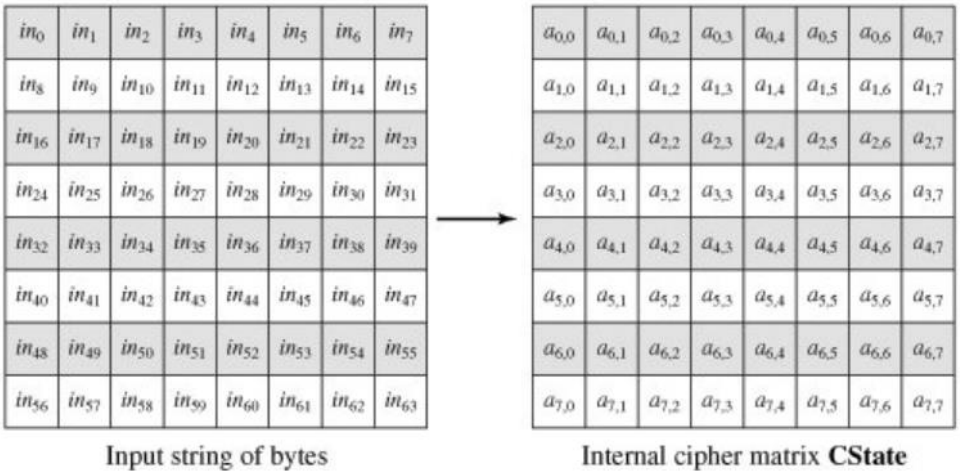


Figure 5: Whirlpool Matrix Structure (Source: Pachghare, (2019) Page 364

Non-Linear Layer of the Byte Substitution

This layer was introduced to establish a non-linear mapping. The resulting bytes from the previous steps form a 16x16 matrix of byte values called S-boxes (SB). The importance of the nonlinearity of this characteristic lies in its ability to provide defense against LnA. The concept behind this layer is to substitute the original bits with predetermined S-box values based on the 16 X 16 matrix of S-boxes. The S-box encompasses a total of 256 distinct values, and these values correspond to specific entries in the matrix when processing input during this layer. To achieve this mapping, row, and column values are assigned to each C-state by extracting the rightmost four digits as the column value and the leftmost four digits as the row value.

(a) S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	18	23	C6	E8	87	B8	01	4F	36	A6	D2	F5	79	6F	91	52
1	60	BC	9B	8E	A3	0C	7B	35	1D	E0	D7	C2	2E	4B	FE	57
2	15	77	37	E5	9F	F0	4A	CA	58	C9	29	0A	B1	A0	6B	85
3	BD	5D	10	F4	CB	3E	05	67	E4	27	41	8B	A7	7D	95	C8
4	FB	EE	7C	66	DD	17	47	9E	CA	2D	BF	07	AD	5A	83	33
5	63	02	AA	71	C8	19	49	C9	F2	E3	5B	88	9A	26	32	B0
6	E9	0F	D5	80	BE	CD	34	48	FF	7A	90	5F	20	68	1A	AE
7	B4	54	93	22	64	F1	73	12	40	08	C3	EC	DB	A1	8D	3D
8	97	00	CF	2B	76	82	D6	1B	B5	AF	6A	50	45	F3	30	EF
9	3F	55	A2	EA	65	BA	2F	C0	DE	1C	FD	4D	92	75	06	8A
A	B2	E6	0E	1F	62	D4	A8	96	F9	C5	25	59	84	72	39	4C
B	5E	78	38	8C	C1	A5	E2	61	B3	21	9C	1E	43	C7	FC	04
C	51	99	6D	0D	FA	DF	7E	24	3B	AB	CE	11	8F	4E	B7	EB
D	3C	81	94	F7	B9	13	2C	D3	E7	6E	C4	03	56	44	7F	A9
E	2A	BB	C1	53	DC	0B	9D	6C	31	74	F6	46	AC	89	14	E1
F	16	3A	69	09	70	B6	C0	ED	CC	42	98	A4	28	5C	F8	86

(b) E mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
E(u)	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

(c) E^{-1} mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E^{-1}(u)$	F	0	D	7	B	E	5	A	9	2	C	1	3	4	8	6

(d) R mini-box

u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
R(u)	7	C	B	D	E	4	9	F	6	3	8	A	2	5	1	0

Figure 6: Whirlpool S-boxes (Source: (Pachghare, 2019)

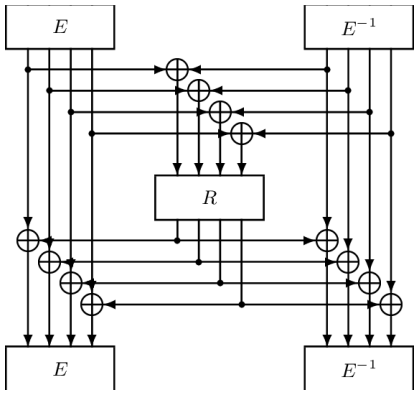


Figure 7: Whirlpool S-box Implementation (Adopted from (Barreto & Rijmen, 2000)

To create S-boxes, two non-linear layers, it is essential to have each S-box containing 4x4 elements. These 4x4 squares are interspersed with randomly generated 4x4 squares. The main objection of these boxes is to associate a 4-bit input with a corresponding 4-bit output. The role of the SB function is to introduce non-linearity into the algorithm. Specifically, the SB function must exhibit no correlation between a linear combination of input bits and a linear combination of output bits. Additionally, changes in sets of input bits should not lead to similar changes across the corresponding output bits. Put differently, even a minor alteration in the input should cause a significant and distinct change in the output. Both of these characteristics enhance the resilience of W against linear and differential cryptographic analysis (Tao & Wu, 2015). This layer has 3 main layers. First is, the SC Permutation Layer, in this layer, the columns undergo a downward circular shift, excluding the first column. Subsequently, the second column undergoes a one-byte shift, the third column undergoes a two-byte shift, and so on. The second is the Diffusion Layer, which is referred to as the diffusion layer, and it incorporates the cryptographic property of diffusion introduced by Claude Shannon (Shannon, 1949). The main objective of this layer is to propagate values by intermixing rows, making the WE Cryptosystem more resistant to LnA. Different value in the product matrix is calculated as the sum of the multiplication of corresponding elements from one column and one row with each element in every row obtained by performing a right circular shift of the preceding row. Lastly, the AK layer, this is to perform the XOR operation between a 512-bit c-state and a 512-bit round key. The results are directed to the W cipher block.

Whirlpool Performance

Comparing Whirlpool to various secure Hash Functions, including all versions of SHA, according to the researchers, Whirlpool demands higher hardware resources but, in return, provides substantially improved throughput (data processing capacity) than SHA-512 (Tao & Wu, 2015). WE are used as a whole in this study because it provides a 512-bit Hash code, the longest among all encryption methods, including MD family cryptographic systems and SHA encryption (Tao & Wu, 2015). It is also resistant to common attacks and weaknesses found in other encryptions, except WE (Gunsing et al., 2020; Sakalli et al., 2014). Moreover, “EW offers better compatibility with hardware and software due to its use of the W block based on AES encryption” (Tao & Wu, 2015). The previous versions of MD family encryption were developed as successors to fix vulnerabilities. For example, MD5 had 2 messages with the same message digest value, rendering it less secure. However, no such issues have been found for WE (Tao & Wu, 2015).

4 Methodology

This research methodology proposes an approach that combines a literature review and a proposed Secure Password Algorithm in access security systems to create passwords with graphical and encryption techniques that are more secure and easy to use. The research started by conducting an in-depth literature review to investigate the weaknesses of the existing graphical and text password methods. The first step of this methodology is to identify the weaknesses of graphical and text passwords that are frequently used in various systems. After these weaknesses are identified, the next research is to develop SPA proposals that focus on using graphical and encryption techniques to increase password security. Furthermore, the research will build the proposed algorithm by considering two main aspects, namely user perception and confidential data security. This algorithm will be designed to create passwords that are not only more secure against common attacks on graphical and text passwords but also easy for users to use. After the algorithm has been built, it will test the performance and security of the algorithm using sample data and appropriate simulation scenarios. This testing will include statistical analysis and observation of user responses to the use of algorithm-generated passwords. This research methodology will also involve surveys or case studies to gather feedback from users using the system with research passwords. This feedback will be used as input for further evaluation and improvement of the proposed algorithm so that more optimal passwords can be generated in terms of security and convenience of use. This research is expected to make a significant contribution to the development of password methods that are more secure and easy to use by combining the literature review and proposed SPA, focusing on graphical and encryption techniques and considering important aspects such as user perception and security of confidential data.

5 Analysis and Results

Password Algorithm “Secure Password Algorithm” (SPA)

The alphanumeric password is hard to remember, so often, users need to look it up again. The solution is graphical ciphers that are easier to remember and more secure (Zhou et al., 2019). Nonetheless, “graphical ciphers are vulnerable to shoulder surfing attacks despite their higher recall than alphanumeric ciphers” (Anuradha et al., 2023). To solve the problem, a new approach is proposed taking into account the human factor. Taking into account the aspect of human perception, SPA creates complex alphanumeric codes through images that are easy to remember. This approach combines the advantages of graphical ciphers and human factors to create a reliable security system that is safe from shoulder surf attacks. Users will be presented with multiple images on the screen, and users can create an image password for each screen according to their preferences. The user will mentally link each image with another associated word. Even if someone could see the user's screen, snoopers wouldn't be able to tell which image was converted to the password because the user didn't select or click on the image. This process involves several secret questions to create a complex and unique password. To safeguard against dictionary attacks, the characters in the password undergo shifting based on a unique number associated with the user's answer. After sliding, the strings are encrypted separately and combined into a large cipher containing 1260 characters. This SPA approach has considered various cyber-attacks such as dictionary attacks, shoulder surf attacks, brute force attacks, and LnA in its development.

Generates Input Strings

To fulfill the Input string, six questions are provided with several image choices that must be responded to by each participant according to the details of the facts and their respective perceptions. For a given image, the user can select a different image/image and provide a response based on perception. Question 1: what do you want to drink now. For example, the image options provided are juice, tea, milk, coffee, and mineral water. Furthermore, users can connect various images or things they want after that followed by the second question, What happy day in your life? The second question appears to be ambiguous and unpredictable. Different individuals may respond with numerical answers, textual explanations, or even something related to their experiences on that particular day, like a received gift. These subjective responses make shoulder surf attacks ineffective since the user does not directly select a specific image in graphical authentication. Instead, they choose an image based on their perception from a pool of available distractions. This approach introduces a high level of randomness, complexity, and difficulty for attackers to discern the user's actual graphical authentication picture during a shoulder surf attack and predict their response based on their perception. Question 3 is What you will choose as an owner business if your product is sold? This is almost the same as the first question, where several are provided randomly and participants must choose and combine stories from the several images presented. Next, question 4 is Write your birthday in DDMMYYYY format so the answer is a number. Continue to question 5 Type the city you like to visit and the year your grandfather passed away, and the participants will write a place name followed by the year number. And finally, the same as question 1 which is Tell me about… (the following image options) where other images are randomly provided again but different from the previously presented, this will allow someone to write anything, short words or long paragraphs. Using these images is an effective way to introduce a high degree of randomness in responses. For example, take the participants' answers randomly from questions 1-7 as "juice", "graduation", "reproduction", "01011998", "Jakarta 1975", "read", and "diversity", and this will be a string: JuiceGraduationReproduction01011998Jakarta1975ReadingDiversity.

Alphabet Shift

This step holds significance as it serves to safeguard against dictionary attacks and LnA. During this process, the number series from the responses to questions 4 and 5 undergo a shift. Specifically, the letters are shifted by the remainder obtained after dividing by 26. Since the answers for questions 4 and 5 are 01011198 and 1975, the calculation for the letter shift will be as follows:

$$\text{Shift} = 01011119981975 \bmod 26 = 22$$

All letters in the resulting string sequence from step 1 will be shifted by 22.

JuiceGraduationReproduction01011998Jakarta1975ReadDiversity

Table 1a: Letter Frequency Analysis (Source: Author Elaboration)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**

Table 1b: Letter Analysis After Shift (Source: Author Elaboration)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	**X**	**Y**	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**

Here, each letter is shifted to twenty-two places and begins with the letter "A" in the rotation. After the shift, the strings become completely different, “Juice Graduation Reproduction 01011998 Jakarta 1975 Read Diversity” namely:

Eqmyacnwzqwpekjnalnkzqgpekj01011998fwgwnpw1975nawzzezanoepu

Divide the String Mentioned Above into Ten Segments

This step is of paramount importance as it directly influences the overall strength of the final password. During the final step, all sections will be encrypted using WE, resulting in each encrypted fragment being converted into a 126-character string. This step permits modifications to either increase or decrease the final password length as needed. WE generate an encrypted string of 126 characters, regardless of the input string's length. Therefore, for randomization, the parts can be divided into any desired proportions. In this case, the sections have been divided into equal parts, the size of the tenth section can vary, being smaller, equal, or larger than the other nine sections because step 2's output might not be a multiple of ten. Table 2 shows the ten parts of our string.

Table 2: Splitting a String into Ten Parts (Source: Author Elaboration)

Segment	Data
1	Eqmyac
2	nwzqwp
3	ekjnal
4	nkzqgp
5	ekj010
6	11998f
7	wgwnpw
8	1975na
9	wzzez
10	anoepu

Encryption of Slices and Composite Output

As discussed earlier, WE assign a unique ciphertext for each input, resulting in a distinct and unique cipher text that serves as our password. The encryption process can be implemented using different programming languages, and numerous websites provide this service at no cost. During step 4, each chunk is individually encrypted to avoid LnA, and subsequently, all the 126-character encryption outcomes are merged to create a 1260-character long password. Step 4 is crucial as it enhances the algorithm's robustness by adding an extra layer of protection against, WE. By encrypting the entire string in separate chunks, as a result, it becomes impractical for an attacker to produce a 1260-character password by encrypting the original string in a single attempt. In WE, every chunk functions as an individual input, and each fragment is encrypted independently, producing ten separate lines of 126 characters each.

Table 3: Encrypted Pieces (Source: Author Elaboration)

Segment	Data	Encrypted Chiper Text
1	Eqmyac	7B592BC402218759B937425E742497806D20454139F19ABEDC73F404CDC3E24F10F32769D0926A0562D5D319FCE21291C88DB0BAE6E12F312712B5282AFF8A41
2	nwzqwp	4CE9A5590B83177FD94906A523DF43FBF73574E5743D15A036C86E2D1D97DFA48EF4DD6B3459E0028EA51B61AC6D5ADDD8670C3D49A 49EA378C7285788BF6CE1
3	ekjnal	B02675B1008AD11620B5011A055515C23F6B53A4355A220B4E0F2604A0D451EAC117D8916899DCABD574E919F4745E9B67EAA9AD48994 B8A5B28D569B56A31D2
4	nkzqgp	D4D02636D3856134E3B95E0247F89FCF2E408C2C614CC93F6FAC2E7BAB9903BC8B43D198E79FDDBE0A018A8E877D7702BB063C220899B DFF5EB7D4E5FF124EA3
5	ekj010	455A4A282FBA8010A91E956021A0F91CBD53481C2279120773D23B06B95B367D2A1763EEB6011989EB3A65E23E1EBE394AAAB8D0442E390AAF5A3FD8FBDFDB76

6	11998f	ADA02278D2EE7BED82A7AF86C0ADF649C00A6D8C8685E5022FDF3D41C358D1CCB54622BC12FA643E58AF8C3C5E368CDD5D8CE639D1 2478E3099F742A7E73CD10
7	wgwnpw	71906328F523016C5D9E2997268E0FEE29429850ED9A0B99F27F95328C9341E1AEFA02622120F175E1E13A821E4D3A9C911B75A41CB2C2E A77174C1643A02AFB
8	1975na	C462C373B5827A247335C72C49712BE86250E9B5EDA0D76D296110EBF9E948E12D416293C4EC16F48213D9C79F2CD56B1993BCDF2AE5B 49541714AD355DFE86D
9	wzzez	5CA12123CA7280553A1F0E7819958C24835777D5C425F02FEEB1CD21EE588498304599DBFAEC08A723575265C5C62D2E9BADA8875B9C53 63B0F6E17FA35AA6C7
10	anoepu	F4118B95A62AD6D51CB1014DD3B50DCD9A476E7698364FD1F9651E01E68AD0A1456414C57CA64F676A5BFCEAFD0B2B72342DFA7CF40

Final Outputs

7B592BC402218759B937425E742497806D20454139F19ABEDC73F404CDC3E24F10F32769D0926A0562D5D319FCE21291C88DB0BAE6E12F312712B5282AFF8A414CE9A5590B83177FD94906A523DF43FBF73574E5743D15A036C86E2D1D97DFA48EF4DD6B3459E0028EA51B61AC6D5ADDD8670C3D49A49EA378C7285788BF6CE1B02675B1008AD11620B5011A055515C23F6B53A4355A220B4E0F2604A0D451EAC117D8916899DCABD574E919F4745E9B67EAA9AD48994B8A5B28D569B56A31D2D4D02636D3856134E3B95E0247F89FCF2E408C2C614CC93F6FAC2E7BAB9903BC8B43D198E79FDDBE0A018A8E877D7702BB063C220899BDFF5EB7D4E5FF124EA3455A4A282FBA8010A91E956021A0F91CBD53481C2279120773D23B06B95B367D2A1763EEB6011989EB3A65E23E1EBE394AAAB8D0442E390AAF5A3FD8FBDFDB76ADA02278D2EE7BED82A7AF86C0ADF649C00A6D8C8685E5022FDF3D41C358D1CCB54622BC12FA643E58AF8C3C5E368CDD5D8CE639D12478E3099F742A7E73CD1071906328F523016C5D9E2997268E0FEE29429850ED9A0B99F27F95328C9341E1AEFA02622120F175E1E13A821E4D3A9C911B75A41CB2C2EA77174C1643A02AFBC462C373B5827A247335C72C49712BE86250E9B5EDA0D76D296110EBF9E948E12D416293C4EC16F48213D9C79F2CD56B1993BCDF2AE5B49541714AD355DFE86D5CA12123CA7280553A1F0E7819958C24835777D5C425F02FEEB1CD21EE588498304599DBFAEC08A723575265C5C62D2E9BADA8875B9C5363B0F6E17FA35AA6C7F4118B95A62AD6D51CB1014DD3B50DCD9A476E7698364FD1F9651E01E68AD0A1456414C57CA64F676A5BFCEAFD0B2B723422DFA7CF40

Computing Speed in Overcoming Passwords

In the present age, computer computing speed is exceptionally high, and it is expected to become even more effective in the next session. Initially, in the past, the computational speed of computers was considerably lower compared to today, but continuous research and advancements have led to significant improvements and improvements in processor technology have led to an exponential increase in computational speed. This rapid speed enhancement has facilitated faster and more efficient password-cracking methods. Over the years, computing speed has shown a remarkable advancement since the early days of computing in the 1900s. Continuous research and advancements in various components of computers are expected to further improve their efficiency and computing power. However, the continuous increase in computing speeds presents a possible danger to the existing password guidelines. Attackers utilize various methods, including the use of computers and botnets, to compromise passwords and breach security systems. As computing speed continues to escalate, it becomes imperative to create strong password-generation methods that can provide enhanced security for computers. Figure 9 illustrates the rapid increase in the Clock Speed of Microprocessors, highlighting the necessity for the development of more sophisticated and challenging password-generation techniques.

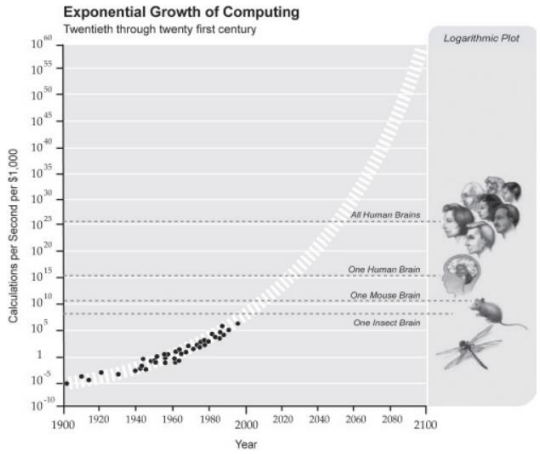


Figure 8: Graph of the Development of Computing Speed (Singularity.com, 2020) Page 70

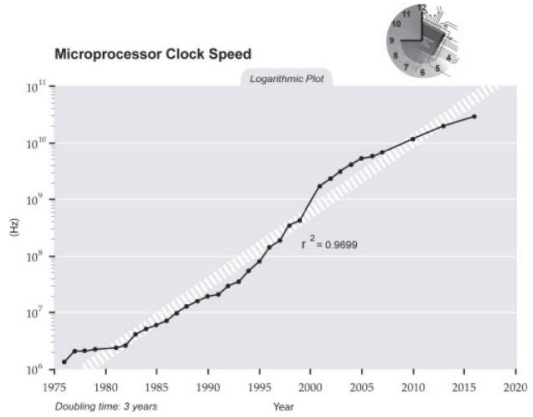


Figure 9: MCS (Source: Singularity.com, (2020) Page 61

The MCS (Microprocessor's clock speed) has been continuously increasing, and the charts demonstrate that it nearly doubles in each 3y. Since 1975, when the clock speed was around 10^6 Hz, extensive research on microprocessors has significantly raised their clock speed. Presently, microprocessor clock speeds have reached almost 10^{11} Hz. Furthermore, improved MCC has consistently led to exponential performance graphs. As computing speed increases, the effectiveness of passwords tends to decrease proportionally.

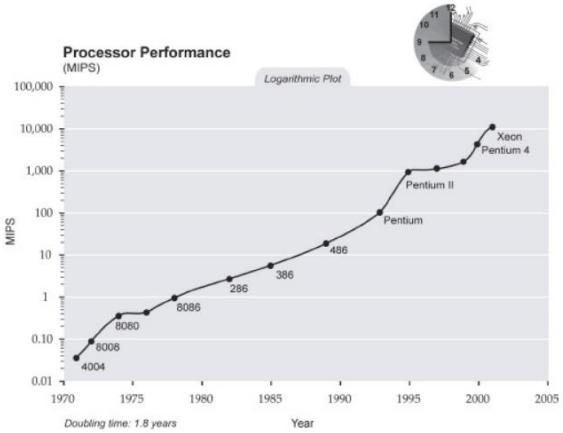


Figure 10: MIPS (Source: Singularity.com, (2020)

The graph illustrates that microprocessor performance nearly doubles approximately every few years. As computers become more sophisticated, passwords must be suitably strengthened to reduce the risk of password compromise using a computer.

Attacks through Modern Computers and Super Computers

At present, no authentication method currently incorporates both graphical authentication (based on human perception) and WE in its authentication process. This research aims to attain elevated levels of security, given the continuous progress in computing power and the ability to jeopardize any authentication algorithm. Although graphical authentication is seldom used, when it is employed, it is usually limited to specific applications like Android applications. Its usage is not widespread due to its vulnerability to SPA. Conversely, encryption methods find extensive application in file security by converting data into an encrypted format and ensuring secure data transfer between different locations. Presently, many websites and applications impose a maximum password length of fifteen characters. These password systems often permit users to create passwords using various combinations. In contrast to this approach, this study emphasizes the role of memory and achieves it through graphical authentication.

Conversely, some social media account recommends users choose passwords that are easily memorable for them but difficult to guess. In such cases, users might write down multiple passwords that, although hard to predict or guess, are highly susceptible to dictionary attacks. Such attacks can compromise all such passwords. Current password rules highlight the variation in password length required for different applications since each application has distinct expectations. At present, authentication is essential for diverse applications, including accessing online Email platforms also emphasize password strength and popular email websites like Gmail.com require users to create passwords of at least eight characters, with a maximum password length of fifteen characters. Gmail also mandates the use of at least one uppercase letter, one lowercase letter, one number, etc., to help users generate more complex passwords. In text passwords, the length and number of characters significantly influence their strength.

Current Password Strength

To demonstrate this SPA, we must consider the computing speed of modern computers employing the SHA512 Hashing algorithm on a modern computer (8 core, 2.8 GHz) consumes around 0,0017ms to calculate the Hash. This corresponds to roughly 1,7 microseconds/password, or the capability to compute 588,235 passwords per second. Different applications allow varying password lengths, spanning from a minimal space to a maximum of ten characters. These applications accept characters from A to Z and 0 to 9To bolster password security, applications should promote longer passwords. The strength of passwords is determined by both the length of the password and the variety of permitted characters. Longer passwords and more character options contribute to stronger passwords due to the increased number of possible combinations. The designed Secure Password Authentication (SPA) has taken into account potential cyberattacks like linear attacks, shoulder peeking attacks, brute force attacks, dictionary attacks, and cryptoanalysis attacks. The proposed SPA is immune to all these types of attacks and has been developed with highly secure WE without any identified vulnerabilities to date. The study and analysis of attacks on current password expectations or rules are essential considering the computing power of modern computers and supercomputers. The SPA's resistance to attacks via modern computers and supercomputers is further demonstrated in this chapter. Attacks on passwords today go through modern and supercomputers.

Attacks Via Modern Computers

Graphical authentication, as researched by (Anuradha et al., 2023), offers superior user memorability, a crucial aspect lacking in current password techniques that rely on alphanumeric passwords. The Secure Password Authentication (SPA) proposed in this study emphasizes the importance of both memorability and high security, exceeding today's password standards. To determine computing speeds, considering the capabilities of modern and supercomputers (100,000 times more efficient than modern computers) is essential. Evaluating the computing speed for the strongest password specifications in modern computers and supercomputers becomes relevant due to the varying specifications of today's password patterns. The maximum time for a current password of fifteen characters in length will be around 1.118987×10^{105} years, found from $1.7 \times 10^{-6} \times 15^{94}$ seconds which is approximately 0.2 times the size of SPA computing speed.

Attack Via Super Computer

Similarly, a supercomputer would take $1.7 \times 10^{-11} \times 15^{94}$ seconds resulting in 1.924111×10^{108} years which is about 20 times shorter than SPA. Thus, the current password will be susceptible to compromise approximately 20 times more quickly than SPA. Assault on the suggested algorithm using contemporary computers (8 cores, 2.8 GHz) and supercomputers.

Attacks Via Modern Computers

To showcase SPA, it is crucial to consider the computational speed of contemporary computers. As previously stated, modern computers require 1.7×10^{-6}s/password. The time needed for SPA to be compromised via modern and supercomputers can be similarly calculated. For SPA, the total computing time on a modern computer would be:

$$\text{Compute speed} = 1.7 \times 10^{-6} \times 1260^{36} = 4.98691 \times 10^{93} \text{ Year.}$$

Hence, modern computers face an almost insurmountable challenge in decrypting these passwords, which takes approximately 21 times longer compared to the computation time of current passwords as mentioned earlier. Thus, it will take a modern computer approximately 21 times longer to decrypt this SPA, making it approximately 20 times more secure than today's standard passwords.

Attacks on Passwords Via Super Computers

By utilizing the given computational speed of the supercomputer, the time required for the supercomputer to attempt a password attack can be calculated like the process used for modern and other supercomputers. The computation time for attacking SPA can be determined as follows:

$$\text{Compute time} = 1.7 \times 10^{-6} \times 1260^{36} \times 10^{-5} = 4.98691 \times 10^{88} \text{years.}$$

These calculations indicate that the total time required to compromise SPA is approximately 20 times longer than the current password standard when attacked by a supercomputer. The Summary table presents a comparison of the current password and SPA from various perspectives.

Table 4: Summary Table Comparing Current Password-generation Solution and Spa (Source: Author Elaboration)

No.	Summary table comparing current password and SPA		
	Comparable Point	**Current Password-generation**	**SPA**
		Main Feature	
1	Intuitive Visual Representation	Depending on the complexity of the characters and length without providing visual support, it is difficult to remember.	SPA menggunakan representasi visual intuitif, seperti pola atau gambar, untuk membantu pengguna membuat kata sandi yang mudah diingat.
2	Adaptability to user preferences.	Current generating password pada umumnya tidak memberikan opsi personalisasi yang luas	SPA memungkinkan pengguna untuk memilih jenis representasi visual dan tingkat kompleksitas yang sesuai dengan preferensi pribad
		Performance metrics	
3	Time for Password Generation	The process of creating passwords in the current password generation takes longer, especially when relying on complex character	Time for Password Generation in SPA significantly reduces the time for password creation through visual representation, resulting in strong passwords more quickly
4	Password Generation	With the current password generation, users have to rely on complex combinations of characters that are difficult to remember, which may take more time and make it challenging for users to recall	To create a strong password with a minimal length, users choose a unique visual representation of SPA. Through quantitative testing, the time required for password generation by SPA can be proven to be shorter compared to traditional solutions, while still providing a high level of security
5	Resistance against attacks	Current password generation is vulnerable to attacks because it relies on conventional characteristics	Single Page Applications (SPAs) demonstrate strong resistance to common attacks, such as brute force attacks, thanks to a combination of visual representation and cryptographic principles.
6	Security Encryption	The security when encryption is performed is quite low	The security when encryption is performed is high
6	Simultaneous authentication	In the Current generating passwords, both graphical and text passwords cannot be used for simultaneous authentication	In SPA, both graphical and text passwords can be used for simultaneous authentication
3	The creation and cracking of passwords	In the current password generation, the creation and cracking of passwords do not depend on multiple confidential pieces of information.	In SPA, the creation and cracking of passwords depend on multiple confidential pieces of information
5	Adequacy	Adequacy only supports 4-15 characters	Adequacy supports up to thousands of characters.
8	Vulnerability to brute force attacks	around 20 times less secure compared to SPA	around 20 times more secure compared to SPA
9	Time required for a computational attack on a modern computer	Less time is required.	Highly secure
10	Time required for a computational attack on a supercomputer	Less time is required.	Highly secure

Therefore, the recently developed SPA offers an improved solution that not only enhances security but also enhances recall ability.

6 Conclusion and Recommendations

Conclusion

This paper examines different graphical authentication methods put forward by other researchers, highlighting the shortcomings and vulnerabilities of each approach. The goal is to find alternatives to text passwords that improve recall. Based on studies, graphical authentication shows the potential to improve memory. Furthermore, this idea was developed taking into account shoulder surfing attacks, where the user only provides perceptual responses without hovering over the image. This makes shoulder surfing attacks difficult for the attacker. This idea also protects the algorithm from dictionary attacks by using the unique user-response character shift concept to generate encryption lines that are difficult for attackers to compromise. This research develops a new encryption algorithm that uses the WE method to encrypt parts of the data. This algorithm effectively addresses the linear attack on the shifted string by dividing it into ten parts and encrypting each part individually via WE. This approach prevents attackers from reaching the final encrypted string by encrypting the original line. Moreover, the algorithm incorporates measures to counter dictionary attacks and brute force attacks from both modern computers and supercomputers. Extensive testing confirms that the algorithm is highly efficient and secure against such attacks. By incorporating user perception, the algorithm gains strength and ease of memorability, and it effectively safeguards against shoulder surfing attacks, which are weaknesses in graphical password methods. Additionally, the proposed SPA can generate passwords up to 1260 characters long based on user-provided perceptions and factual details. Each data chunk is encrypted into a 126-character string, and the combined encrypted results create a robust defense against brute-force attacks from modern computers and supercomputers, making it nearly impossible for them to crack.

Research Advice

This research investigates SPA in depth but still has room for technical development. Software implementation has not been done completely automatically. In the future, software can be implemented to increase efficiency and save time. In addition, psychometric, psychological, and psychiatric studies can help better understand user perceptions and protect systems from attacks. Tests such as the Rorschach test can be used to improve understanding of user input based on their perceptions.

References

[1] Anuradha, M., Loganathan, S., Suseela, G., Selvan, M.P., & Nalini, M. (2023). Hybrid Multiple Cryptography for Data Encryption. *In IEEE 8th International Conference on Communication and Electronics Systems (ICCES)*, 596-603.

[2] Barreto, P.S.L.M., & Rijmen, V. (2000). The Whirlpool hashing function. In *First open NESSIE Workshop, Leuven, Belgium, 13*, 1-20.

[3] Blömer, J., & May, A. (2004). A generalized Wiener attack on RSA. In *International Workshop on Public Key Cryptography*, 1-13. Berlin, Heidelberg: Springer Berlin Heidelberg.

[4] Brostoff, S., & Sasse, M.A. (2000). Are Pass faces more usable than passwords? A field trial investigation. *In People and computers XIV—usability or else! Proceedings of HCI*, 405-424. Springer London.

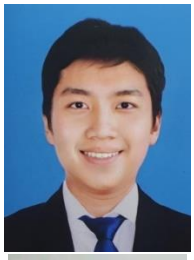
[5] Buriro, A., Gupta, S., Yautsiukhin, A., & Crispo, B. (2021). Risk-driven behavioral biometric-based one-shot-cum-continuous user authentication scheme. *Journal of Signal Processing Systems, 93*, 989-1006.

[6] Cockell, R., & Halak, B. (2020). On the design and analysis of a biometric authentication system using keystroke dynamics. *Cryptography*, *4*(2), 1-14.
[7] Craik, F.I., & McDowd, J.M. (1987). Age differences in recall and recognition. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, *13*(3), 474-479.
[8] Deane, F., Barrelle, K., Henderson, R., & Mahar, D. (1995). Perceived acceptability of biometric security systems. *Computers & Security*, *14*(3), 225-231.
[9] Dee, T., Richardson, I., & Tyagi, A. (2022). Continuous nonintrusive mobile device soft keyboard biometric authentication. *Cryptography*, *6*(2), 1-24.
[10] Gokhale, A., & Waghmare, V. (2014). A Study of Various Passwords Authentication Techniques. *International Journal of Computer Applications*, *975*, 1-5.
[11] Grammatopoulos, A.V., Politis, I., & Xenakis, C. (2022). Blind software-assisted conformance and security assessment of FIDO2/WebAuthn implementations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *13*(2), 96-127.
[12] Gunsing, A., Daemen, J., & Mennink, B. (2020). Errata to sound hashing modes of arbitrary functions, permutations, and block ciphers. *IACR Transactions on Symmetric Cryptology*, 362-366.
[13] Ho, Y.L., Lau, S.H., & Azman, A. (2021). Comparison of BlindLoginV2 and Audio Blind Login with the common textual password authentication for the blind and visually impaired using smartphones. *International Journal of Human-Computer Studies*, *156*.
[14] Islam, A., Othman, F., Sakib, N., & Babu, H.M.H. (2023). Prevention of shoulder-surfing attacks using shifting condition using digraph substitution rules. *Artificial Intelligence and Applications*, *1*(1), 58-68.
[15] Jayapal, R. (2017). Biometric encryption system for increased security, 1-46.
[16] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., & Rubin, A. (1999). The design and analysis of graphical passwords. *In 8th USENIX Security Symposium (USENIX Security 99)*.
[17] Jiang, X., Liu, X., Fan, J., Ye, X., Dai, C., Clancy, E.A., & Chen, W. (2021). Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. *IEEE Internet of Things Journal*, *8*(22), 16535-16547.
[18] Kenneth, M.O., & Olujuwon, S.M. (2021). Web Application Authentication Using Visual Cryptography and Cued Clicked Point Recall-based Graphical Password. *Journal of Computer Science Research*, *3*(3), 29-41.
[19] Khudhur, D.Y., Hameed, S.S., & Al-Barzinji, S.M. (2018). Enhancing e-banking security: using whirlpool hash function for card number encryption. *International Journal of Engineering and Technology*, *7*(2), 281-286.
[20] Nam, S., Jeon, S., Kim, H., & Moon, J. (2020). Recurrent gans password cracker for IoT password security enhancement. *Sensors*, *20*(11), 1-19.
[21] Nguyen, T.A., & Zeng, Y. (2010). A vision based graphical password. *Journal of Integrated Design and Process Science*, *14*(2), 43-52.
[22] Nyirongo, R., Kuonga, S., Ali, P., Eneya, L., & Kim, H. (2017). Cryptanalysis and Enhancement of Password Authentication Scheme for Smart Card. *International Journal on Cryptography and Information Security*, *7*(3), 1-13.
[23] Pachghare, V.K. (2019). *Cryptography and information security*. PHI Learning Pvt. Ltd.
[24] Rui, Z., & Yan, Z. (2018). A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access*, *7*, 5994-6009.
[25] Sakallı, M.T., Akleylek, S., Aslan, B., Buluş, E., & Sakallı, F.B. (2014). On the construction of and binary matrices with good implementation properties for lightweight block ciphers and hash functions. *Mathematical Problems in Engineering*, *2014*.
[26] Shannon, C.E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.
[27] Sharma, A.K., & Mittal, S.K. (2020). Cryptographic keyed hash function: PARAŚU-256. *Journal of Computational and Theoretical Nanoscience*, *17*(11), 5072-5084.

[28] Singularity.com. (2020). Singularity is Near -SIN Graph - Micro Processor Clock Speed. Singularity.Com. https://www.singularity.com/charts/page61.html
[29] Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M.S., & Kumar, V.M. (2011). Authentication schemes for session passwords using color and images. *International Journal of Network Security & Its Applications, 3*(3), 111-119.
[30] Tao, B., & Wu, H. (2015). Improving the biclique cryptanalysis of AES. In *Information Security and Privacy: 20th Australasian Conference, ACISP, Brisbane, QLD, Australia, Proceedings 20*, 39-56. Springer International Publishing.
[31] Tippannavar, S.S., Yashwanth, S.D., & Madappa, E.A. (2023). Two Factor Authentication using RFID and Biometric sensor–A Progressive Review. *International Journal of Advanced Research in Computer and Communication Engineering, 12*(6), 261-271.
[32] Wang, B., Wu, W., Zhang, Y., & Zhang, L. (2023). New Integral Distinguishers on Permutation of Whirlpool. *The Computer Journal*.
[33] Zhou, Z., Yang, C.N., Yang, Y., & Sun, X. (2019). Polynomial-based Google map graphical password system against shoulder-surfing attacks in cloud environment. *Complexity, 2019*, 1-8.

Authors Biography

Joseph Teguh Santoso was born in Surabaya, Indonesia in 1981. He obtained his Bachelor of Informatics Engineering (S. Kom) at STIKUBANK University, graduating in 2002. In 2004, he received his Master of Informatics Engineering (M. Kom) at Dian Nuswantoro University (UDINUS), and his Doctor of Philosophy (Dr) degree at Indonesian Theological College Jakarta received in 2019. He is the Rector of the University of Science & Computer Technology (STEKOM University) in Semarang and has a lot of practical experience in the field of e-commerce since 2002. He owns three official online stores in China for the Raleigh bicycle brand and holds the exclusive license for the "Raleigh" bicycle brand for online sales throughout China. In addition, he also owns a bicycle and electric bicycle factory under the "Fengjiu" brand, which is a relatively small electric bicycle factory in China.



Budi Raharjo was born in Semarang, Indonesia, in 1985. He is a graduate of Bina Nusantara University (BINUS University) as S. Kom in Jakarta and Satya Wacana Christian University (UKSW) as a Master of Information Systems (M. Kom) in Salatiga. He received his Master of Management (M. M) from Satyagama University Jakarta and his Dr or Ph. D from STTI Jakarta. He is a lecturer at STEKOM University and serves as the Vice Rector 1 for academic affairs.

Agus Wibowo holds Ph. D degrees from Diponegoro University (UNDIP) in Semarang and Satya Wacana Christian University (UKSW) in Salatiga. His disciplines include electrical engineering, computer science, management, and sociology. With work experience in the electronics industry, he holds certifications in Internet Networking, Telecommunications, Artificial Intelligence, Internet of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing, and data processing and analysis (computer statistics). Agus Wibowo also holds the position of Associate Professor, producing numerous textbooks with ISBN, Intellectual Property Rights (HAKI) for several creative works, and patents for technological products. He is actively involved in various professional and industry organizations related to business and industry, particularly in the development of outstanding human resources to meet the real-world needs of the job market.