Mesopotamian journal of Cybersecurity
Vol.5,No.2, **pp**. 491–500
DOI: https://doi.org/10.58496/MJCS/2025/030; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

A Secure Password based Authentication with Variable Key Lengths Based on the Image Embedded Method

Seerwan Waleed Jirjees,[1], Farah Flayyeh Alkhalid [1], Ahmed Mudheher Hasan [1], Amjad Jaleel Humaidi [1,*]

[1] *College of Control and Systems Engineering, University of Technology- Iraq, Baghdad 10066, Iraq.*

ARTICLE INFO

Article history

Received 24 Nov 2024
Revised 21 Mar 2025
Accepted 17 May 2025
Published 17 Jun 2025

Keywords

Authentication
Man in Middle Attack
Image Encryption
Text Encryption
Secure Password

ABSTRACT

Passwords are widely used to secure client–server communication in authentication-based systems that are used over untrusted transmission media; thus, users' passwords are vulnerable, and systems are vulnerable to hacking. In this paper, we propose a new philosophy for secret password encryption where encryption is secure between communicating parties during a communication session while ensuring resistance to man-in-the-middle attacks and preventing dictionary attacks in violation of trustworthiness without relying on trusted third parties or other out-of-band mechanisms for authentication, which will be encrypted on the basis of the data from the image sent during authentication. The proposed encryption scheme will encode each character of the password and replace it with a value representing the pixel value locations in the image and choose randomly. The sent image serves as the key to the algorithm used to encrypt the password after encrypting it with the same password. The proposed approach provides security, efficiency, reliability and cryptanalysis against various attacks. The proposed scheme has shown ability through several security analyses to resist man-in-the-middle attacks and reattacks. Finally, we compare the performance of our protocol with that of existing schemes. Hence, our system ensures good security and efficiency features.

1. INTRODUCTION

Password-based authentication is the most widespread method used in various systems and applications to verify the identities of users [1, 2]. The security of password-based authentication depends on the set of measures implemented by the system to protect passwords from unauthorised access [3, 4]. To mitigate these risks, various techniques have been developed, such as enforcing password complexity rules, implementing multifactor authentication, using password hashing and salting, updating passwords regularly, and educating users about password security [5-7]. However, password-based authentication has inherent limitations and weaknesses, such as brute force attacks, social engineering attacks, and dictionary attacks [8, 9].

Ensuring password security during transmission is of paramount importance to protect sensitive information from unauthorised access. To achieve this, several measures should be implemented. Firstly, passwords should always be transmitted over secure channels via encryption. Different encryption algorithms are used to secure the transmission of passwords and data. If it is eavesdropped and the encryption algorithm is simple, there is a chance that the password will be decrypted and stolen [10][36]. There are many ways to prevent man-in-the-middle attacks in the context of secure end-to-end communication, but they rely either on trusted third parties or on custom solutions primarily built on traditional cryptographic systems, aimed at allowing end users to verify the authenticity of public keys. These methods do not provide a high degree of ease of implementation as well as security [11-13].

Loss of security between the two parties occurs by deceiving both parties by using the wrong key if the key exchange process with the third party is not secure [14-16].We propose a password encryption algorithm between two entities without relying on a trusted third party or other out-of-band mechanisms for authentication by depending on relying on images sent between the two parties and encrypting them with a key that represents the password with an agreed-upon encryption algorithm and then relying on the encrypted image data to encrypt the password, which ensures its resistance to man-in-the-middle attacks in a way that cannot be analysed or known by hackers. Our paper's contributions can be outlined through the following key points:

*Corresponding author. Email: amjad.j.humaidi@uotechnology.edu.iq

1. The proposed system introduces a unique authentication method for password encoding on the basis of the pixel locations of the image sent by the server.
2. Several criteria determine the effectiveness of this approach, as it will depend on the randomness of the images used, their size, the type of algorithm employed for encryption, and the randomness in selecting the password character encoding from the pixel locations of the encrypted image.
3. To increase the security of the password during transmission and its resistance to man-in-the-middle attacks, even if the passwords are intercepted, attackers will still need the transmitted image and its encryption method to crack the password data. It is worth noting that the image will change with each new connection.

The remainder of the paper is organized as follows. In Section 2, a brief review of previous works is given. Section 3 presents the proposed algorithm for the system and describes how it works. Section 4 includes the analysis and experimental results. In Section 5, some conclusions are presented with key future ideas.

2. RELATED WORKS

Many studies have focused on the authentication process, especially in recent years; however, online transactions are among the main transactions in our daily activities. Eko et al. [17] suggested a new method to improve the safety of information transmitted by using a quadric key producer model, in which the model expected cyberattacks by producing quadric keys before encryption. It involves quadric producers, a random key producer, a key flow producer, a key scheduling producer, and a random pseudo-numerical algorithm producer. On the other hand, in the decoder section, the system produces triple keys before decryption to confirm information secrecy and to sidestep cyberattacks. Ahmet et al. [18] proposed a unique method for saving sensitive online data for the password-based encryption approach. In this method, there is no password file to manage the verification process. To create encryption/decryption keys, a one-way hash function is employed with the user's entered password, the unique salt value acquired from the proposed system database during registration, and the number of iterations. They used the “PBKDF2WithHmacSHA1” algorithm to create the key through “AES/CBC/PKCS5 Padding” selection to encode the password with 1000 iterations. In [19], the authors developed a dynamic password generator that depends on character frequencies by matching the frequencies of digits, characters, and special characters to zero in a hash table and then calculating the threshold of each character in a way that makes it uniform. After the threshold is checked by a flag, a user will construct a password by choosing characters from good characters that are less than the threshold. This approach involves fast time processing and saves from attackers.

Lin et al. [20] proposed an algorithm based on solving the problem in the Hwang--Yeh scheme, which is that the password protocol change may be attacked and does not have a secret redirection to pass the key. Lin et al. developed a password modification protocol starved of key distributions to prevent denial-of-service attacks depending on the Diffie Hellman key exchange approach and advised the length of the password characters (8--14). The authors of [21] proposed a novel algorithm for password encryption: first, the user should fill in (first name, last name, email, and date of birth (DOB)), then calculate the square root of the DOB summation (day, month, and year), then obtain the round and choose the two digits after the floating point as a base, after which the equivalent binary to the users password is found, and finally, the encryption value is calculated. They advised that the length of the password should not exceed 11 characters since the base value and the effects of creating the encrypted password.

The authors of [22] proposed an elliptical curve cryptography, which involves reverting the plaintext to equivalent ASCII, then collecting the ASCII numbers, transforming them to large numbers by multiplying ASCII with b numbers. The large numbers correspond with the following large numbers and creating a pair, which is denoted as appoint, to create the encryption key. The authors of [23] presented a hybrid security layered model; this model guaranteed the safety of the information, and therefore, the information safety was conserved. The authors suggested several structural blocks, and these blocks were subjected to hashing and encryption. The plain text was divided into several blocks and tracked by a tree constructed. This was followed by the calculation of hash ciphers, which was completed via the keccak-256 hash codes. These codes were encoded by the Advanced Encryption Standard (AES) 256, with a varying key generated by CodeIgniter.

Panahi et al. [24] focused on the importance of encryption in Internet of Things (IoT) devices that transfer sensitive data that must be nearby only by permitted authorities. The main goal of low-power devices is to create a light block for encryption projection by dropping the number of successive series and memory, and the latter aims to reduce energy feeding and memory convention. There are 25 circles in the proposed encryption, which contains the following stages: AddRoundKey (a simple bitwise XOR (Of round subkey) applied to the intermediate state), SubColumn (parallel application of S-boxes to the four bits in the same column), and ShiftRow (a left rotation applies to each row over different offsets).

Compared with previous studies, this paper proposes an encryption algorithm for authentication data. This algorithm is not based on the key or its size, as in previous studies; however, the password can be changed and updated according to a predefined protocol between the sender and receiver, as shown in the next section.

3. THE PROPOSED SYSTEM

The proposed system aims to protect the password during the authentication process, which is encrypted on the basis of random images stored in advance in the server database and sent to the client randomly when a connection is requested. The proposed system, as shown in Figure 1, employs a method in which the password is not encrypted directly using an encryption algorithm; instead, the password characters are encoded on the basis of data from an image sent by the server after being encrypted. The password encryption in the proposed system changes the character value using the coordinates of the pixel values (row, column) of the image sent by the server. The image received by the user will be encrypted by an algorithm that is agreed upon in advance, with the password serving as the key the algorithm uses to encrypt the image. The image size and type will vary with each new communication session, as it will be randomly selected. Figure 2 illustrates how the proposed authentication scheme operates in a multiuser environment.

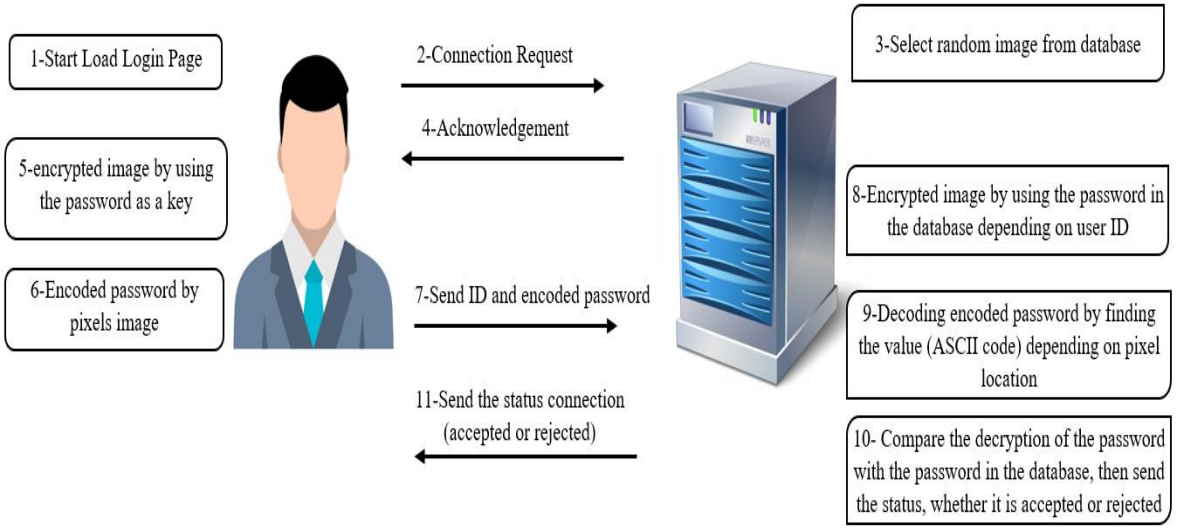

Fig. 1. A simple scenario of authentication

The proposal involves two principles: a server S who is responsible for user authentication and who sends a randomly selected image to client U, who requests the service from the application server. The proposed system uses an authentication technique that consists of two phases: the registration phase and the authentication phase (login phase). Table I shows the abbreviations used in the description and algorithms below:

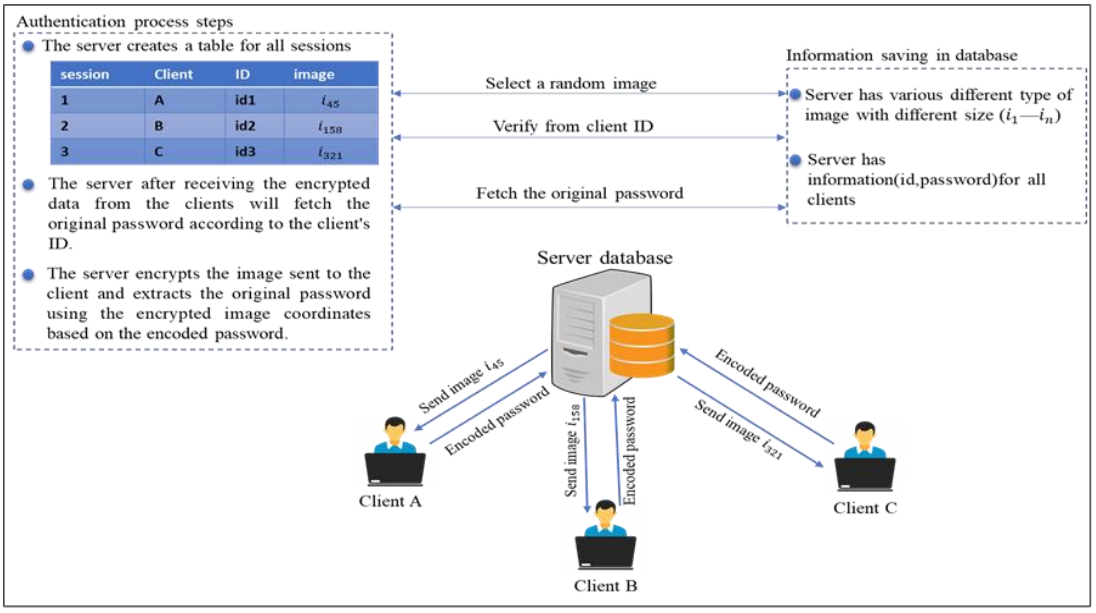

Fig. 2. Multiuser authentication for the proposed system

TABLE I. ABBREVIATIONS

Abbreviation	Details
U	User
S	Server
ID	User id
CI	Cipher text
IM	Original image
EA	Encrypted image
PW	password
()	location value in array
[]	content value of location in an array
&	Append two String

3.1 Registration phase

The user requests that the server sign up, which can be described as follows.

Step 1 U → S: {ID, PW}

- The user selects his/her identity (ID) and password (PW) to register and sends them with secure channels.

Step 2 S → U: {IM, EA}

- The server sends a random image (IM) and the encryption algorithm technique (EA) to encrypt the image after checking the ID if it does not exist; otherwise, go to step 1.

Step 3 U → S: {ID, EP}

- The user applies the encoding proposed system that is illustrated in Algorithm 1 and then sends the ID and ciphertext (EP).

Step 4 S → U: Sending the registration status (rejection or acceptance).

3.2 Authentication phase

As shown in Figure 1, the user requests that the server log, which can be described as follows.

Step 1 U → S: request login page.

Step 2 S → U: {IM, EA}

- The server sends a random image via an encryption algorithm.

Step 3 U → S: { ID, PW }

- The user enters his/her ID and enters the password (PW).
- An encryption algorithm is applied to the encrypted image using PW as a key.
- (C) is created by converting the ASCII code for each character to the location of the pixel.

Step 4 S → U: {IM, EA}

- The server checks the availability of the ID in the database if decryption is executed in the proposed system to convert cipher text to alphanumerical text and then compares it with a plaintext password that is saved in the database; otherwise, go to step 1.
- The server starts encrypting the image with the key and the same encryption algorithm and then compares.

Step 5 S → U: Registration rejection or registration success

- Depending on step 4, if the password matches, the connection is established; otherwise, authentication is rejected.

3.3 Encryption algorithm

The encryption algorithm described consists of three levels, as illustrated in Figure 3.

First Level: ASCII Code Conversion. At this level, each character in the password is independently converted into its corresponding ASCII code.

Second Level: Greyscale image conversion and encryption. At this level, the image is converted to greyscale, and then the greyscale image is encrypted via a preagreed-upon encryption algorithm. This work focuses on an ordinary image encoding method using a one-key symmetric algorithm, which can be performed through the use of various methods.

Third Level: Random Indexing for ASCII Codes. At this level, each ASCII character obtained at the first level is encoded with coordinates (row and column). The encoding process is performed by searching for an ASCII value in the table obtained at the binary level and choosing one of the values randomly. The purpose of using random indexing is to add an extra layer of randomness to the encryption process, making it more difficult to decrypt without a key or a suitable decryption algorithm.

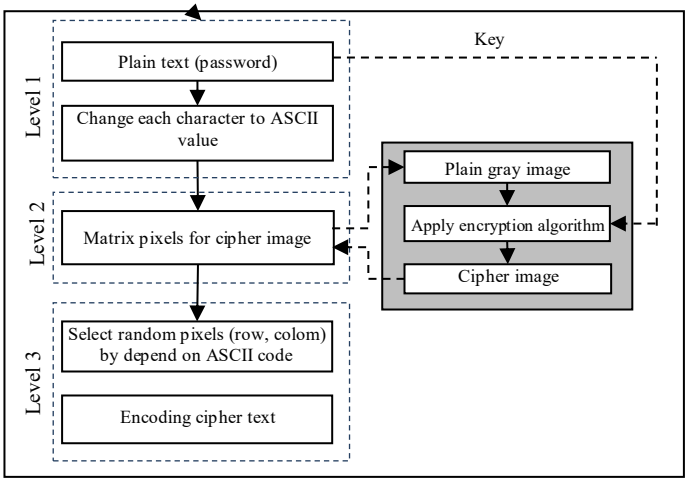

Fig. 3. The proposed algorithm

The proposed encryption strategy typically relies on converting the ASCII code of the password characters into coordinates from a value randomly selected from the pixel corresponding to the ASCII code of the encrypted image data. Algorithm 1 illustrates these steps.

Algorithm 1: Encryption proposed algorithm

Input : Plain image I of size x×y×3 password PW=(t_0,t_1,…., t_z) where t=alphanumerical and z=length of PW

Output: Cipher text P

1: convert the input image I to a grayscale image.
2: apply the encryption algorithm for M
3: create matrix (f[x,y]) for cipher image
4: For i =1 to z /loop to read the characters
5: convert character M[i] to ASCII code (II)
6: TA= all locations(f[x,y]) of II /where TA=temporary array
7: RV = random location from TA
8: P[i]+= RV
9: End For i

For example, let the password be "CoM19$", and the image size is 10 × 8, as shown in Table II. The process begins by converting each password letter into an ASCII code. In the second stage, a table is generated from the data of the encrypted image. Then, each ASCII value in the array is searched, where it searches for the number 67, which represents the letter C, randomly selects one of the positions between (1,7) and (8,4), then moves to the number 111, which represents the letter o, and chooses one of the positions (4,7), (5,3), (8,8) randomly. The same process is repeated for all characters of the password until an encrypted password is obtained, which in our example is (2,8,5,3,5,1,2,9,8,9,3,3,3).

TABLE II. CHARAYCTER ENCODING OF COORDINATE VALUES

Plain Character	Level 1	Level 2 The matrix for grayscale encrypted image									Level 3
			1	2	3	4	5	6	7	8	9	
	ASCII	1	30	56	120	198	218	202	190	252	9	Location
C	67	2	65	194	35	7	56	123	63	67	49	[2, 8]
o	111	3	182	15	92	35	57	128	77	41	98	[5, 3]
M	77	4	116	103	35	118	93	55	111	21	57	[5, 1]
		5	77	143	111	35	90	75	18	103	13	
1	49	6	214	178	50	147	224	30	113	174	16	[2, 9]
9	57	7	18	49	27	67	34	73	56	132	48	[8, 9]
		8	176	80	222	3	240	63	14	111	57	
$	35	9	13	0	119	104	1	47	201	63	11	[3,3]

3.4 Decryption algorithm

The decryption process is performed as described in Algorithm 2. First, the transmitted image is encrypted according to

the chosen algorithm by the password stored in the server databases. In the next step, the process of decoding the ciphertext begins by reading the row and column numbers and finding the pixel location value from a matrix of the encoded image, which represents the ASCII code for the character. Finally, the comparison process will take place with the text obtained from the decryption process with the password in the database, and depending on the result, a decision will be made to agree to grant permission to enter or to refuse the connection.

Algorithm 2: The proposed of the decryption algorithm

Input **:** Plain image I of size x×y×3 ,cipher text CI=(t_0,t_1,…., t_z) where t=alphanumerical and z=length of CI, original text V loaded from database

Output**:** plain text P

1: Convert the input image I to grayscale image.
2: Apply encryption algorithm R(x,y) to ER(x,y)
3: For i=0 to z step 2
4: ch=ER [t_i, t_{i+1}]
5: P[i]=convert ASCII to character (ch)
6: End for
7: If V=p then
8: Op=" connection acceptance"
9: Else
10: Op=" connection rejected"
11: End if

4. ANALYSIS AND SECURITY

The proposed encryption algorithm, which is based on the RSA cryptography system, is conducted on the Python platform and uses a computer system. The processor is manufactured with Intel core i5-3110 M, the CPU is 2.40 GHz, the RAM is 16.00 GB, the hard disk drive is 500 GB, and the operating system is 64-bit Windows 11. Figure 4 shows the security and effectiveness of the proposed technique in preserving the confidentiality of the sent password from the attacker's attempt to hack it.

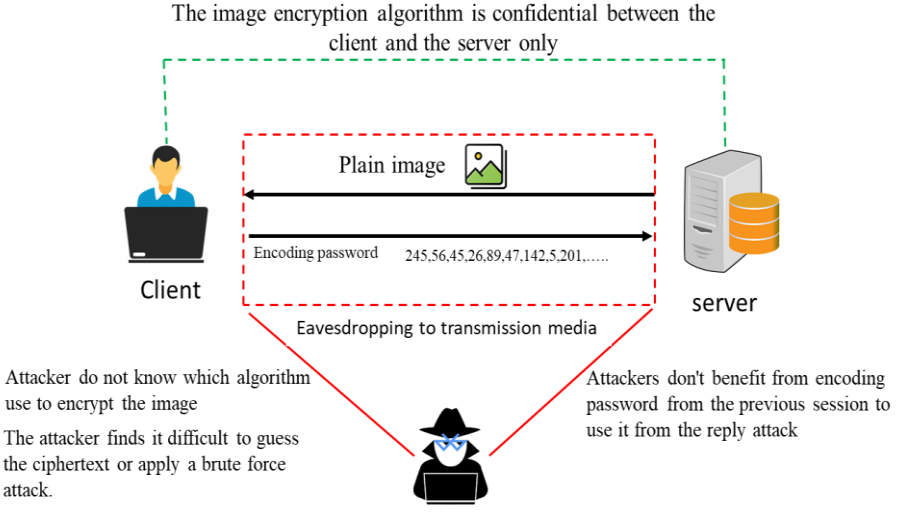

Fig. 4. The proposal's ability to resist types of attacks

4.1 Encryption Time

The proposed algorithm time depends on the time required to encrypt the image and is based on the type of algorithm used, the size of the image, and the length of the password characters. Table III shows the estimated time required to encrypt information according to the size and type of algorithm used to encrypt the image.

TABLE III. ENCRYPTION TIME IN THE SECOND

Password Length	Image size		
	255×255	512×512	1024×1024
8 char	0.043	0.109	0.422
12 char	0.046	0.111	0.439
16 char	0.048	0.120	0.469

4.2 Eavesdropping Attack

In this type of attack, attackers illegally listen to the confidential information exchanged between the client and server [25, 26]. The data encryption process depends on a set of basic elements, such as the algorithm used to encrypt the image and the random selection of pixels used to encode the data. In addition to the random selection of the size and type of image, the attacker cannot benefit from the encrypted data stolen from another connection because the image has changed and the coding happens randomly, so the algorithm resists this type of attack.

4.3 Replay Offensive

The attacker copies the message stream that needs to be transmitted between two parties to retransmit it later with the intent of gaining unauthorized access and impersonating the user [27]. This type of attack is resisted because the ciphertext is reencoded with each new login by changing the image, and even if the same image is used, the encryption algorithm relies on randomly encoding characters. Thus, if the attacker sends the intercepted text, the attacker will be unable to connect and detect the retransmission attack.

4.4 Known Plaintext Attack

In this type, the attacker accesses a copy of the original text and the ciphertext in an attempt to discover the algorithm used in encryption or to find the secret key. In the proposed scheme, the secret key used to encrypt the password is variable, it depends on randomly selected images, and the algorithm also uses a random method to encode the password characters from the image data [28].

4.5 Avalanche Property Key Sensitivity Analysis

It is a cryptographic concept where a small change in the input value (message) creates a large change in the output, and traditional encryption algorithms use the text with the key to form the ciphertext. Sometimes, when only one bit is changed, there will be similarity in the ciphertext [29, 30]. For the proposed algorithm, the characters of the original text will not be directly involved in the encryption process but will be replaced by random values represented by numbers. In the proposed system, the image changes in each connection request process, therefore, the values are variable according to the transmitted image information and the randomness in choosing the values. In Table IV, one letter of the word was changed, and it was encoded on the same image and of different sizes.

TABLE IV. AVALANCHE EFFECT PROPERTY: THE NUMBER OF BITS CHANGED IN THE CIPHERTEXT WITH NO CHANGES IN THE IMAGE PROPERTIES (255×255)

Session	Plain text	Cipher text
First	aaaaaa	245,56,45,26,89,47,142,5,201,19,178,105
Second	aaaaaa	8,15,141,1,23,240,19,139,70,8,19,20
Third	aaaaaa	15,16,209,226,8,4,12,150,12,190,17,209
First	Hello	37,0,9,147,172,33,97,147,28,58,142,30
Second	Hello	143,123,45,17,1,155,70,4,213,50,18,115
Third	Hello	49,32,147,7,12, 3,1,9,230,129,247,73

4.6 Possible Combinations of Brute Force

To decrypt the ciphertext, cryptanalysts use a brute-force attack method, which is based on the size of the key space, which represents the number of possible possibilities that can be used in the cipher [31, 32]. In the proposed encryption algorithm, the password is encoded using data from the encrypted image. The probability of finding the total number of attempts for the correct password (TA) in the proposed approach can be determined as shown in equation (1).

$$TA=2^{(x\times y)}\times L \quad (1)$$

where L represents the length of the password (x, y) represents the row column of the image. This equation allows for an estimate of the number of attempts required to decrypt the ciphertext, which can help to determine the strength of the encryption algorithm. It is large enough to resist all kinds of brute-force attacks.

4.7 Algorithm Encryption Strength

To calculate the efficiency and encryption strength of the proposed algorithm, several criteria are used to calculate the extent of the effect of the algorithm used on the ciphertext and compare it to the original text; below are the criteria used to measure the performance of the proposed method.

- **In histogram analysis**, the histogram represents the even distribution of input values [31]. The values that make up the ciphertext are random numbers chosen from the image coordinates that change in each connection**,** and their values depend on the size of the image. The histogram distribution of the coordinate values does not necessarily have to be equal, even if the same coordinates are repeated in the password encryption, because it depends on the randomness of the choice**,** and these values change with each new connection.
- Entropy is a measure of the randomness of the values in the ciphertext [32]. In our algorithm, the randomness of the resulting numbers does not affect the strength of the ciphertext because these numbers represent the content of values that change in each communication process. In other words, its content is variable even if the ciphertext numbers are repeated.
- The correlation coefficient is the extent of similarity in values between the original text and the ciphertext because, in most traditional methods, the original text is part of the encryption algorithm, which is necessary for these algorithms to calculate the extent of similarity [33]; however, this criterion does not apply to the proposed algorithm because the original text does not enter directly into the encryption process.

5 COMPARISON

This section compares the proposed algorithm to password-based authentication algorithms and methods, as well as how to keep them safe while they communicate. We focus on security standards and methods that make the comparison less likely to be attacked. Table 4 presents the results of the comparison with the following algorithms: multifactor authentication (MFA), public key authentication (SSH Keys), and transport layer security (TLS) [34-35]. Our proposed algorithm is better at protecting against brute force attacks than are the other algorithms. This is because password encryption relies on a large and variable image size that represents the key in traditional encryption methods and is chosen randomly. The algorithm used to encrypt images is not specified. Nevertheless, it requires additional costs by providing memory in the database to store images, and the time to encrypt images and encode them takes longer than encrypting text followed in other algorithms. The authentication system in the SSH method requires exchanging keys before starting the password encryption process via the asymmetric encryption algorithm, and the STL method requires three-factor authentication and the MFA algorithm, which is vulnerable to phishing and social engineering attacks. For our proposed algorithm, we do not need a third party or key exchange, and the password is not directly entered into the encryption algorithm, which gives the proposed algorithm the ability to resist all types of attacks.

TABLE V. COMPARISON BETWEEN THE PROPOSED AUTHENTICATION ALGORITHM AND DIFFERENT AUTHENTICATION ALGORITHMS.

Metric	TLS	SSH	MFA	Proposed System
Usability	Complex (need third party)	Simple (exchange keys)	Complex (method to verify one-time password)	Simple (just send an image)
Key exchange	Yes	Yes	Yes	No
Computational cost	Exchange keys	Exchange keys	Use a One-Time Password (OTP) method such as SMS.	Direct encryption using the password as a key
Authentication connection	Indirect connection (client -certificate authority-server)	Direct connection (client-server)	Indirect connection (Example: Email Service Providers or Biometric Authentication Providers)	Direct connection (client to server)
Encryption type	asymmetric & symmetric	asymmetric	asymmetric	symmetric
Transfer cost	Low (Just keys are transferred as values)	Low (Just keys are transferred as values)	High (Depend on the type of authentication like SMS, fingerprint or voice recognition.	Medium (Depends on the size of the images sent)

6. CONCLUSION

The proposed system aims to ensure the confidentiality of passwords sent during the authentication process via a unique approach that does not include direct encryption of the plain text or the use of a third party for authentication. The original text will not be encrypted but will be a key to encrypt the image sent by the server to obtain random numbers that are

different from the original image, as each letter of the password will be encrypted on the basis of the pixel locations of the encrypted image. Notably, the algorithm has succeeded in achieving a set of strong points:

- Generate encrypted text from encrypted image information.
- Security depends on three elements (password type, image size, and image type).
- It is difficult for an intruder to discover the methods used to encrypt an image.
- The password letter symbols in the secret text are completely different

The numerical results of the relationship between the original password and the encrypted password prove that the resulting data are completely different from the original data and that attackers cannot find useful information in the encrypted text.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

None.

Acknowledgement

None

References

[1] W. Ding, N. Wang, P. Wang, and S. Qing, "Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity," *Inf. Sci.*, vol. 321, pp. 162–178, 2015, doi: 10.1016/j.ins.2015.03.070.

[2] A. T. Ali, H. Abdullah, and M. N. Fadhil, "Impostor recognition based voice authentication by applying three machine learning algorithms," *Iraqi J. Comput. Communun. Control Eng.*, vol. 21, no. 3, pp. 112–124, 1970, doi: 10.33103/uot.ijccce.21.3.10.

[3] S. A. Sheikh and M. T. Banday, "Multi-recipient e-mail messages: Privacy issues and possible solutions," *Adv. Electr. Comput. Eng.*, vol. 21, no. 4, pp. 115–126, 2021, doi: 10.4316/AECE.2021.04013.

[4] S. W. Jirjees, A. R. Nasser, and A. M. Mahmood, "RoundPIN: Shoulder surfing resistance for PIN entry with randomized keypad," *Int. J. Secur. Softw. Eng.*, vol. 11, no. 6, pp. 697–702, 2021, doi: 10.18280/ijsse.110610.

[5] X. Jiang et al., "Neuromuscular password-based user authentication," *IEEE Trans. Ind. Inform.*, vol. 17, no. 4, pp. 2641–2652, Apr. 2020, doi: 10.1109/TII.2020.3001612.

[6] L. A. Salman, A. T. Hashim, and A. M. Hasan, "Automated brain tumor detection of MRI image based on hybrid image processing techniques," *TELKOMNIKA Telecommun. Comput. Electron. Control*, vol. 20, no. 4, pp. 762–771, 2022, doi: 10.12928/telkomnika.v20i4.22760.

[7] S. W. Jirjees, F. F. Alkhalid, and A. M. Hasan, "Text encryption by indexing ASCII of characters based on the locations of pixels of the image," *Traitement du Signal*, vol. 40, no. 2, pp. 791–796, 2023, doi: 10.18280/ts.400240.

[8] A. K. Jabbar, A. T. Hashim, and Q. F. Al-Doori, "Secured medical image hashing based on frequency domain with chaotic map," *Eng. Technol. J.*, vol. 39, no. 5A, pp. 711–722, 2021, doi: 10.30684/etj.v39i5A.1786.

[9] A. T. Hashim, A. M. Hasan, and H. M. Abbas, "Design and implementation of proposed 320 bit RC6-cascade encryption/decryption cores on Altera FPGA," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6370–6379, 2020.

[10] M. Kim and T. Suh, "Eavesdropping vulnerability and countermeasure in infrared communication for IoT devices," *Sensors*, vol. 21, no. 24, p. 8207, 2021, doi: 10.3390/s21248207.

[11] S. E. Yunakovsky et al., "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technol.*, vol. 8, p. 14, 2021, doi: 10.1140/epjqt/s40507-021-00104-z.

[12] P. Wlazlo et al., "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," *IET Cyber-Phys. Syst.: Theory Appl.*, vol. 6, no. 3, pp. 164–177, Jun. 2021, doi: 10.1049/cps2.12014.

[13] L. A. Salman, A. T. Hashim, and A. M. Hasan, "Selective medical image encryption using polynomial-based secret image sharing and chaotic map," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 3, pp. 357–369, 2022.

[14] C.-T. Chen, C.-C. Lee, and I.-C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *PLOS ONE*, vol. 15, no. 4, p. e0232277, 2020, doi: 10.1371/journal.pone.0234631.

[15] H. Dalkilic and M. H. Ozcanhan, "A strong mutual authentication protocol for securing wearable smart textile applications," *Adv. Electr. Comput. Eng.*, vol. 22, no. 1, pp. 31–38, 2022, doi: 10.4316/AECE.2022.01004.
[16] N. A. Hasan and A. K. Farhan, "Security improve in ZigBee protocol based on RSA public algorithm in WSN," *Eng. Technol. J.*, vol. 37, no. 3B, pp. 67–73, 2019, doi: 10.30684/etj.37.3B.1.
[17] E. H. Riyadi, T. K. Priyambodo, and A. E. Putra, "The dynamic symmetric four-key-generators system for securing data transmission in the industrial control system," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 1, pp. 376–386, Feb. 2021, doi: 10.22266/IJIES2021.0228.35.
[18] A. F. Mustacoglu, F. O. Catak, and G. C. Fox, "Password-based encryption approach for securing sensitive data," *Security Privacy*, vol. 3, no. 5, Sep. 2020, doi: 10.1002/spy2.121.
[19] A. Singh and S. Raj, "Securing password using dynamic password policy generator algorithm," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1357–1361, Apr. 2022, doi: 10.1016/j.jksuci.2019.06.006.
[20] C. L. Lin and T. Hwang, "A password authentication scheme with secure password updating," *Comput. Security*, vol. 22, no. 1, pp. 68–72, 2003, doi: 10.1016/S0167-4048(03)00114-7.
[21] S. Roy, S. M. Siddiquee, M. K. Rahman, and A. Al Marouf, "A novel authentication method for password encryption," in *Proc. 4th Int. Conf. Electron., Commun. Aerospace Technol. (ICECA)*, 2020, pp. 780–785, doi: 10.1109/ICECA49313.2020.9297542.
[22] D. Natanael, Faisal, and D. Suryani, "Text encryption in Android chat applications using elliptical curve cryptography (ECC)," in *Proc. Int. Conf. Comput. Sci.*, Elsevier B.V., 2018, pp. 283–291, doi: 10.1016/j.procs.2018.08.176.
[23] M. B. Jayalekshmi and S. H. Krishnaveni, "TSS - Twin layered security scheme for cloud storage to preserve data integrity," *Int. J. Intell. Eng. Syst.*, vol. 10, no. 3, pp. 94–101, Jun. 2017, doi: 10.22266/ijies2017.0630.11.
[24] P. Panahi, C. Bayılmış, U. Çavuşoğlu, and S. Kaçar, "Performance evaluation of lightweight encryption algorithms for IoT-based applications," *Arab. J. Sci. Eng.*, vol. 46, no. 4, pp. 4015–4037, Apr. 2021, doi: 10.1007/s13369-021-05358-4.
[25] W. Yang et al., "Security analysis of a distributed networked system under eavesdropping attacks," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 67, no. 7, pp. 1254–1258, Jul. 2019, doi: 10.1109/TCSII.2019.2928558.
[26] D. Vukovic Grbic, Z. Djuric, and A. Kelec, "Enhancing security and privacy in modern text-based instant messaging communications," *Adv. Electr. Comput. Eng.*, vol. 24, no. 2, pp. 49–60, 2024, doi: 10.4316/AECE.2024.02006.
[27] S. Yu et al., "A secure and efficient three-factor authentication protocol in global mobility networks," *Appl. Sci.*, vol. 10, no. 10, p. 3565, 2020, doi: 10.3390/app10103565.
[28] S. Zhu and C. Zhu, "An efficient chosen-plaintext attack on an image fusion encryption algorithm based on DNA operation and hyperchaos," *Entropy*, vol. 23, no. 7, p. 804, 2021, doi: 10.3390/e23070804.
[29] B. P. Kumar and E. S. Reddy, "An efficient security model for password generation and time complexity analysis for cracking the password," *Int. J. Saf. Secur. Eng.*, vol. 10, no. 5, pp. 713–720, 2020, doi: 10.18280/ijsse.100517.
[30] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Process.*, vol. 171, p. 107484, 2020, doi: 10.1016/j.sigpro.2020.107484.
[31] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020, doi: 10.1109/ACCESS.2020.2989050.
[32] S. W. Jirjees and F. F. Alkhalid, "IMGTXT: Image to text encryption based on encoding pixel contrasts," *Math. Model. Eng. Problems*, vol. 9, no. 2, pp. 539–544, 2022, doi: 10.18280/mmep.090233.
[33] L. A. Salman, A. T. Hashim, and A. M. Hasan, "Selective medical image encryption using polynomial-based secret image sharing and chaotic map," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 3, pp. 357–369, 2022, doi: 10.18280/ijsse.120310.
[34] Z. ur Rahman et al., "Generative adversarial networks (GANs) for image augmentation in farming: A review," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3505989.
[35] K. Yazid, H. Ibrahim, and M. Z. Abdullah, "Enhanced patchwise maximal intensity prior for deblurring neutron radiographic images," *Int. J. Electr. Comput. Eng. Syst.*, vol. 16, no. 2, pp. 133–152, 2025, doi: 10.32985/ijeces.16.2.5.
[36] A. S. Abdul-Zahra, E. Ghane, A. Kamali, and A. A. F. Ogaili, "Power forecasting in continuous extrusion of pure titanium using Naïve Bayes algorithm," Terra Joule Journal, vol. 1, no. 1, Art. no. 2, 2024. [Online]. Available: https://tjj.researchcommons.org/journal/vol1/iss1/2