УДК 004.056.52
МРНТИ 81.93.29

TWO FACTOR AUTHENTICATION USING TWOFISH ENCRYPTION AND VISUAL CRYPTOGRAPHY ALGORITHMS FOR SECURE DATA COMMUNICATION

G. DUISEN[1], A. RAZAQUE[1], ZH. SEITKALIYEVA[1], R. YESTAYEVA[1], FATHI AMSAAD[2]

[1]International Information Technology University
[1]University of Southern Mississippi, Mississippi, USA

Abstract: *The growing dependence of human needs on the Internet has pleased the need for secure and confidential processing of data on the World Wide Web. Therefore, the safe processing of information entails the need for speed and availability of systems. Improving the reliability and privacy of systems directly depends on a fully protected authentication method. There are various authentication and protection methods that have been developed to ensure confidentiality and security. Their main part is based on an alphanumeric password, and only a small part is classified as two-factor authentication. In this article, we offer an improved graphical authentication method based on Twofish Encryption algorithm and Visual Cryptography (TEVC). The proposed TEVC is organized in such a way that it is impossible to predict the correct graphic password, and is further complicated by the fact that for authentication it is necessary to present its correct order, which makes it safer than an alphanumeric password.*
TEVC was developed and tested in the programming language JAVA. After testing, we can argue that the proposed authentication method satisfies the necessary security requirements. TEVC has been identified as a convenient and secure authentication method with less time complexity compared to other known authentication methods.

Keywords: *Twofish encryption, visual cryptography, encryption, graphical password, alphanumeric password system, authentication method, two factor authentication*

TWOFISH ШИФРЫ МЕН ВИЗУАЛДЫ КРИПТОГРАФИЯНЫҢ НЕГІЗІНДЕГІ АҚПАРАТТЫ ҚАУІПСІЗ ӨҢДЕУГЕ АРНАЛҒАН ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯ ӘДІСІ

Аңдатпа: *Адамзаттың Интернетке зәрулігінің артуы дүниежүзілік өрмекте ақпаратты қауіпсіз және құпия өңдеу қажеттілігін тудырды. Сондықтан ақпараттың қауіпсіз өңдеу жүйенің жылдам және қолжетімді болуын талап етеді. Жүйенің сенімділігі мен құпиялылығының деңгейі оның аутентификация әдісіне тікелей байланысты. Құпиялылық пен қауіпсіздікті қамтамасыз ету үшін пайда болған түрлі аутентификация әдістер бар. Олардың негізгі бөлігі әріптік-сандық құпия сөзге негізделген, тек біраз бөлігі ғана екі факторлы аутентификация ретінде жіктеледі. Осы мақалада біз Twofish шифрлау алгоритмі және Визуалды Криптография (TEVC) негізіндегі графикалық аутентификация әдісін ұсынамыз. Біздің пайымдауымызша, TEVC дұрыс графикалық парольді болжау мүмкін болмайтындай етіп ұйымдастырылып, аутентификация үшін оның дұрыс ретін көрсету қажеттілігімен қиындатылған, бұл оның әріптік-сандық парольге қарағанда, қауіпсіз болуын қамтамасыз етеді.*
TEVC JAVA программалау тілінде әзірленді және сыналды. Тексеруден кейін көрсетілген аутентификация әдісі қажетті қауіпсіздік талаптарын қанағаттандырады. TEVC басқа танымал аутентификация әдістерімен салыстырғанда ыңғайлы және уақыттың күрделілігінің аздығымен сенімді аутентификация әдісі ретінде анықталды.

Түйінді сөздер: *Twofish шифрлау, визуалды криптография, шифрлау, графикалық пароль, әріптік-сандық пароль жүйесі, аутентификация әдісі, екі факторлы аутентификация*

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ ШИФРОВАНИЯ TWOFISH И ВИЗУАЛЬНОЙ КРИПТОГРАФИИ ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ

Аннотация: *Рост зависимости человеческих нужд от Интернета породил необходимость безопасного и конфиденциального процессирования данных в мировой паутине. Следовательно, безопасная обработка информации влечет за собой необходимость быстроты и доступности систем. Повышение надежности и конфиденциальности систем напрямую зависит от полностью защищенного метода аутентификации. Существуют разные методы аутентификации и защиты, которые были разработаны для обеспечения конфиденциальности и надежности. Их основная часть базируется на буквенно-цифровом пароле, и лишь маленькая часть классифицируется как двухфакторная аутентификация. В этой статье мы предлагаем улучшенный графический метод аутентификации на основе Алгоритма шифрования Twofish и Визуальной Криптографии (TEVC). Предлагаемый авторами TEVC организован так, что невозможно предугадать правильный графический пароль, и дополнительно осложнен тем, что для аутентификации необходимо предъявить правильный его порядок, что делает его надежнее буквенно-цифрового пароля.*

TEVC был разработан и протестирован на языке программирования JAVA. После проведения тестирования можно утверждать, что предлагаемый метод аутентификации удовлетворяет необходимым требованиям безопасности. TEVC был определен как удобный и безопасный метод аутентификации с меньшей временной сложностью по сравнению с другими известными методами аутентификации.

Ключевые слова: *шифрование Twofish, визуальная криптография, шифрование, графический пароль, система буквенно-цифровых паролей, метод аутентификации, двухфакторная аутентификация*

I. INTRODUCTION

The world of technology and IT infrastructure development has increased the impact on people's daily lives. At the moment, several services are provided via the Internet. Thus, authentication in this environment is difficult to perform. On the other hand, identity verification was a significant problem. Over time, the number of successful attacks, including security breaches and identity fraud, is increasing. Thus, secure password authentication is required. [1]. The paper [2] introduced numerous user authentication methods, such as password, token, PIN codes, certificates and biometrics, which are divided into different categories: what the user knows, what the user has, who he is. One of the widely used methods is the alphanumeric password system, since it is a simple, inexpensive and convenient mechanism for use and implementation. Despite its popularity, the system has its drawbacks.A previous study shows that users typically choose short alphanumeric passwords that are easy to remember. However, this is easy to guess. On the other hand, if a complex password is selected, then it is more difficult to guess the alphanumeric password. But it is often difficult to remember. Since users can only remember a limited number of alphanumeric passwords. But often they write down passwords or use the same password for several accounts. Also, attackers can gain easy access to private and confidential data by cracking passwords. There are many attacks aimed at hacking the password method; such as brute force attack, dictionary attack, rainbow table attack, etc. The graphic password was developed as an alternative to the alpha-numeric password. The incentive for a graphical password is that users can memorize pictures better than text. Human psychology supports this assumption. Because of this advantage of memorization, there is a conditional interest in the graphic password [3].

Single-factor authentication can be broken by known methods, such as phishing, social engineering, and brute-force attacks, therefore, the likelihood of theft and impersonation of credentials increases. Thus, significant counter-measures were applied on the server side to combat misidentification in the authentication system. One of the known authentication methods is

two-factor authentication (2FA) [4]. A common possible basis for the authentication factor in 2FA systems is a one-time password (OTP). The main reason for combining OTP with another component of verification is that there is a possibility of theft or loss of an OTP generation device [5]. Using this technique in conjunction with an alphanumeric password, taking into account the limitations and limitations of both authentication methods, we conclude that this integration does not provide an adequate level of security, although this technique is widely used.

Another possible 2FA method is fingerprint scanning in combination with a regular password. This method is widely used in most consumer smartphones. However, users are still concerned about this method, the reason is to use the high cost of integration. Since this limitation is associated with the replacement of fingerprints and the lack of recovery methods [6].

As for the weaknesses of 2FA technology, a new authentication structure method is proposed. The user identity verification system will consist of a graphical password and visual cryptography in combination with the Twofish encryption algorithm. Visual cryptography is a method of encrypting general confidential information: data about the original solitary image is shared between two or more images (shared images). Interpretation is carried out by simple superposition of common images and does not require calculations, like some optical logic circuits [7]. Thus, the system checks the user with an unorganized graphical password, which is a completed version of visual cryptography. It is initially embedded with an encrypted keyword. Compared to an alphanumeric password, the method must correspond not only to the order of the graphic password, but also to the encrypted keyword in the graphic password. Due to the fact that the keyword is encrypted with the Twofish encryption algorithm embedded in the image, visual cryptography is used. Thus, the possibility of predicting the encryption algorithm for sequential hacking is excluded.

This paper consists of the following contributions:

• The authentication system is provided to the user in the form of a graphical user interface and does not allow attackers to know the backend of the algorithm;

• Unordered selection of parts of pictures to hide a keyword reduces the likelihood of hacking;

• Since the images for authentication are stored on the local device, the possibility of replacing the user ID in the system is excluded;

• Since a graphic password does not have a fixed pattern, predicting the correct order is an obstacle for a potential intruder.

The remainder of this document is organized as follows: Section II discusses the definition of the problem and its significance. Section III presents the essential features of the existing work. Section IV suggests Twofish encryption and visual cryptography. Section V shows the experimental setup and results, and finally, the entire article ends in Section VI.

II. PROBLEM IDENTIFICATIONAND SIGNIFICANCE

The notional concern exists in authentication systems. As it is utilized not just for security of PCs in conventional sense, but also for control of access to cell phones, houses, ATMs and numerous other. Frequently passwords are the main security connected to the application against unapproved access. But unfortunately, numerous users are not completely mindful of significance of passwords. They routinely build up the short, effectively memorable passwords which are helpless for the attacks. Notwithstanding parcel of study has been directed on reinforcing of passwords, however information are as yet powerless against hazard all the time. In this manner, there is need of secure passwords for users just as to associations. As, the criminal can hack the database of the site where enrollment information of the client are put away and to unveil a colossal number of passwords. Thefts can likewise occur at the individual level. The user can compose the password some place, and it can fall into hands of criminals. Besides, the client can set basic and simple password which can be speculated. The social engineering, a phishing or keyloggers can

be connected to endanger passwords. Passwords can be regularly misused by brute force or the dictionary attack in an independent mode [8].

The investigation provided in [9] discusses about that from March, 2016 till March, 2017 were uncovered 788,000 potential casualties of a keylogging. Subsequently, 12.4 million potential casualties of a phishing and 1.9 billion login names of the clients and passwords progressed toward becoming injured individual because of information rupture. The observation demonstrates that the break of enlistment information and a phishing which influenced the exploited people in the United States and Europe, while keyloggers excessively impact on the unfortunate casualties in Turkey, on Philippines, in Malaysia, Thailand and Iran.

As the outcomes of previously mentioned assaults on a one-factor password framework, the association or individual can encounter individual and private huge misfortune to individual and associations. While looking these password constraints and hacking difficulties, there is need of strong password insurance technique that shields the passwords from being hacked as well as gives the easy method for memorizing the password.

III. RELATED WORK

In this segment, the striking highlights of existing work are outlined. Secure Online Transaction Algorithm is presented in [10] uses 2FA together with OTP. Statistics were uncovered that around 18 million adults were victims of identity theft in the United States in 2014. To reduce dangers followed by these infringement an algorithm Secure Online Transaction Algorithm (SOTA) was proposed. When the Consumer chooses the items in the online administration and continues to checkout, SOTA will start to give security. The consumer enters credit card number and charging address. The online store asks for information entered by the Consumer to the credit card company utilizing standard Public Key Infrastructure Advanced Encryption Standard (PKI AES) encryption. PKI AES enables client to rapidly send data from the online store to the charge card company. When the data is affirmed, the credit card organization sends an arbitrarily produced eight-digit number to the online seller and to consumer's telephone application using the PKI.This random code is encrypted by secure hash algorithm This random code is encoded by secure hash algorithm (SHA-256 hash). This limits the likelihood that an unapproved client may utilize another person's data to make deceitful buys. Without a legitimate code, criminals can't utilize the stolen card to make buys. The upside of this algorithm is that it gives security of both the buyer and credit card companies, which may endure monetary harm. The weakness of this algorithm is the utilization of slow hash technique SHA-256.

2FA method of image-based passwords utilizing pictures and random questions is exhibited in [11] examines the memorizing password issue of a regular authentication method. This investigation proposed a two-factor a preauthentication procedure of image-based passwords utilizing images and random questions. The registration procedure for the authentication framework occurred as following: the user chooses an image and answering the given 5 questions. At that point, at the authentication framework, the user needs to pick the photos that he picked throughout the registration procedure and answer the 3 questions.If the data matches, then access is allowed. The following measurement was uncovered: when the third login was performed (15 days after registration), the level of successful logins on our proposed work was 95% contrasted with 58.33% of the alphanumeric password. The upside of the proposed technique is capacity to forestall the assault of surfing on the shoulders. As a drawback, the untrustworthiness of answer to the questions technique was uncovered.

Two Factor Authentication Using Visual Cryptography and Digital Envelope in Kerberos is presented in [12] recommended a 2FA algorithm that utilizes Kerberos and Visual Cryptography. Kerberos is the framework dependent on the tickets in which the Key Distribution Center (KDC) shares a ticket, ciphered by a client password, and the client decodes it to get a ticket on other network services. To expand the secure level of Kerberos, the algorithm was adjusted by including the idea

of visual cryptography and a digital envelope. For this reason, message exchange between the user and KDC was altered, precisely Ticket Granting Ticket request and encryption plan of conventional Kerberos convention were transfigured. The framework profited with utilizing Visual Cryptography, AES and Digital Envelope. Furthermore, it was inclined to replay and dictionary attack. Disadvantage is the likelihood of Man-in-the-middle attack on KDC.

Advanced smart card based password authentication protocol is introduced in [13] discusses about progress of smart card authentication system proposed by Xu-Zhu-Feng. This paper talks about potential attacks on the Xu-Zhu-Feng's system and recommends upgrades to avert disadvantages. Proposed new productive strong smart card based password authentication protocol which fulfills the requirements of effectiveness and reciprocal authentication. The benefit of the proposed protocol is capacity of reciprocal validating both server and client in the meantime. In this manner, common confirmation forestalls server side impersonation.

S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme is presented in [14] discusses vulnerability of textual and graphical passwords. S3PAS is intended for use in client-server systems as most password validation frameworks. Proposed framework produces the login picture locally and transmits the picture particular. S3PAS effectively incorporates both graphical and textual password schemes and gives close ideal protection from attacks from a strong camera, concealed cameras and spyware. It can supplant or exist together with normal text password frameworks without changing existing client password profiles. Additionally, it is safe to savage power assaults through unique and unstable secret key sessions. S3PAS indicates significant potential conquering any hindrance between regular textual password and graphical password.

BioHashing is very tolerant of information catch counterbalances with a similar user fingerprint data, resulting in high bit chain correlation. In addition, there is no deterministic method to get user code without a token with random information and a user ID function. This will secure us, for instance, from biometric invention by changing the user credentials is as simple as changing the token containing the random information. BioHashing has significant functional privilege over purely biometric markers, that is, a zero equivalent point error rate and a perfect detachment of real and deceitful populaces, which dispenses with the likelihood of false gatherings, without experiencing an expansion in the quantity of false deviations.

IV. PROPOSED TWOFISH ENCRYPTION AND VISUAL CRYPTOGRAPHY

Most of the known authentication frameworks depend on alphanumeric password. Accordingly, these techniques cause the remembering and hacking the password issues. The proposed TEVC algorithm gives a helpful and secure technique for validation to the system. TEVC operates on conjunction of Twofish encryption algorithm and Visual Cryptography described in algorithm 1.

Algorithm 1: The User-adding process to the system

1. Initialization: (G: Graphical Password; GP: Graphical password particles; UGP: User ordered graphical password particles, K: keyword; EK: Encrypted Keyword, UAO: User Authentication Object)
2. Input: (G, UGP, K)
3. Output: (GP, UAO)
4. divide G into six particles to get GP
5. get EK by encrypting K by Twofish
6. get UAO by Visual Cryptography in UGP using EK
7. save in database

In algorithm 1, step 1 shows the initialization process of components such as graphical password, graphical password particles, user ordered graphical password particles, keyword, and encrypted keyword. In steps 2-3, input and output are shown respectively. In step-4, the im-

age is splintered into six graphical password particles. These particles are represented in term of 3x2 matrix UGP:

$$UGP = [x_{11}x_{12}x_{13}x_{21}x_{22}x_{23}] \quad (1)$$

where $x_{11}(i = 1,2,3;\ j = 1,2)$ are each graphical password particles. Thus, the complexity of proposed method is increased against possible attacks. For exposing the system to the threat of an account hacking, a selection of all possible options (APO) is needed:

$$APO = n! \quad (2)$$

where in our case, $n = 6$

For GP, in order to permute its rows and columns, we generate matrix of image particles in ascending order:

$$GP = UGP(floor(APO*x_i))modi, \quad (3)$$

where $x_i \in UGP$, i =3, 2, 1

By this implies we can guarantee the components in GP are the permuted line numbers without repetition.

For passwords produced by a user that arbitrarily chooses a s string of symbol of length, L, from a lot of C possible symbols, the quantity of possible passwords can be found by raising the quantity of symbols to the power L:

$$K = C^L \quad (4)$$

Where 'K' is the keyword chosen by the user; L is the length of the password, and 8≤L ≤15; and C is the complexity of the password. Since our system require uppercase (A-Z), lowercase (a-z) letters, numbers (0-9), and special characters as !"#¤%&/\()=+-:*, complexity value 'C' will raise to 77. The proposed system has advantage of constraints on keyword inputted by user. Furthermore, it is difficult to crack a password consisting of random characters. Random password resists guessing attacks due to the high entropy and brute force attacks because there are many characters.

Next, the way toward requesting graphical password particles by the user is performed. Along these lines, the User requested UGP is acquired. In stage 5, input keyword is encrypted by Twofish. Stages 6-7 describe the procedure of integration of the graphical password and encrypted key utilizing visual cryptography that is finally spared in the database. The graphical representation of user-adding process is delineated in Figure 1.

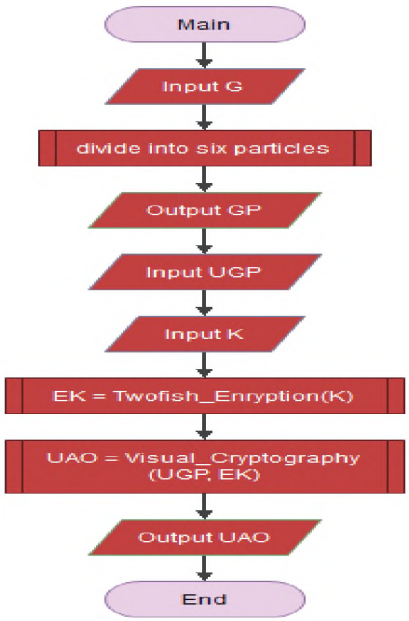

Figure 1- User adding process in the system

The keyword is converted to to bits and divided into 4 parts, 32 bits each. These are: L0, L1, R0, R1.

$$L0' = K0 \ \text{Å} L0 \quad (5)$$

$$L1' = K1 \ \text{Å} L1 \quad (6)$$

$$R0' = (R0 \ \text{Å} K2) \ \text{Å} (K_{2r+8} + PHT(g(L0'))) \quad (7)$$

$$R1' = ((R1 \ \text{Å} K3);1) \ \text{Å}(K_{2r+9} + PHT(g(L1';8))) \quad (8)$$

where, r is round number and K0, K1, K2, K3, K_{2r+8}, K_{2r+9} are keys for encryption that are generated dynamically.

'g' and PHT (Pseudo-Hadamard transformation) are internal functions of Twofish algorithm. The '*g*' function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on Maximum Distance Separable (MDS) matrix. PHT is reversible transformation of a bit line which provides cryptographic diffusion.

These equations repeat 16 times. Afterwards, EK:

$$EK = (K4Å\ R1') \,||\, (K5\ Å\ R0') \,||\, (K6\ Å\ L0') \,||\, (K7Å\ L1') \quad (9)$$

where, K4, K5, K6, K7 are keys.

Upon completion of the processing of Algorithm 1, registered users are stored in the database as a sequence:

$$U = \{U_1, U_2, U_3, \ldots, U_n\} \quad (10)$$

where U_i indicates each user registered in the system.

Algorithm 2: Authentication using TEVC

1. **Initialization:** {UAO: User Authentication Object; EK: encrypted keyword; DK: decrypted keyword; CK: correct keyword, AS: Authorization status, U: User}
2. **Input:** {UAO}
3. **Output:** {U}
4. Set AS = 0
5. if UAO -- then
6. extract EK by Visual Cryptography
7. get DK by decrypting EK using Twofish Encryption Algorithm
8. if DK == CK then
9. set AS = 1
10. endif
11. endif
12. if AS == 1 then
13. U = valid
14. user granted authorization
15. elseif
16. U = invalid
17. endif

In algorithm 2, step 1, shows initialization process of used variables. Steps 2-3 explain the input and output processes respectively. In step 4, program checks the right order of User ordered UGP as stored in database. If the graphical password verification process succeeds, in step 5, the system retrieves the encrypted keyword from the UGP by using the visual cryptography. In step 6, described the process of decryption of the keyword In algorithm 2, stage 1, demonstrates instatement procedure of utilized factors. Stages 2-3 clarify the input and output operation respectively. In stage 4, program checks the correct order of User ordered UGP as put away in database. In the case that the graphical password checking process succeeds, in stage 5, the system recovers the encoded keyword from the UGP by utilizing the visual cryptography. In stage 6, shown the procedure of decryption of the keyword extracted from the graphical password by utilizing Twofish algorithm. Checking of condition if the decrypted keyword matches right keyword from the database procedure is described in stage 7. On the off chance that the condition is met, stage 8 sets authorization status value to 1. Stages 11-16 explain the checking procedure of authorization. On account of authorization, status value equivalents to 1, authorization is granted to the user. Otherwise, a user isn't considered as authorized. The authentication and authorization process is delineated in Figure 2.

The registration of the user starts with adding an image into the system:

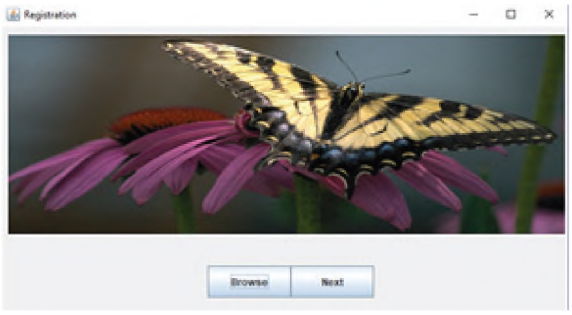

Figure 3 – image adding

The system divides image into six particles:

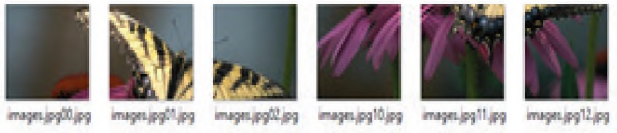

Figure 4 – particles of graphical password

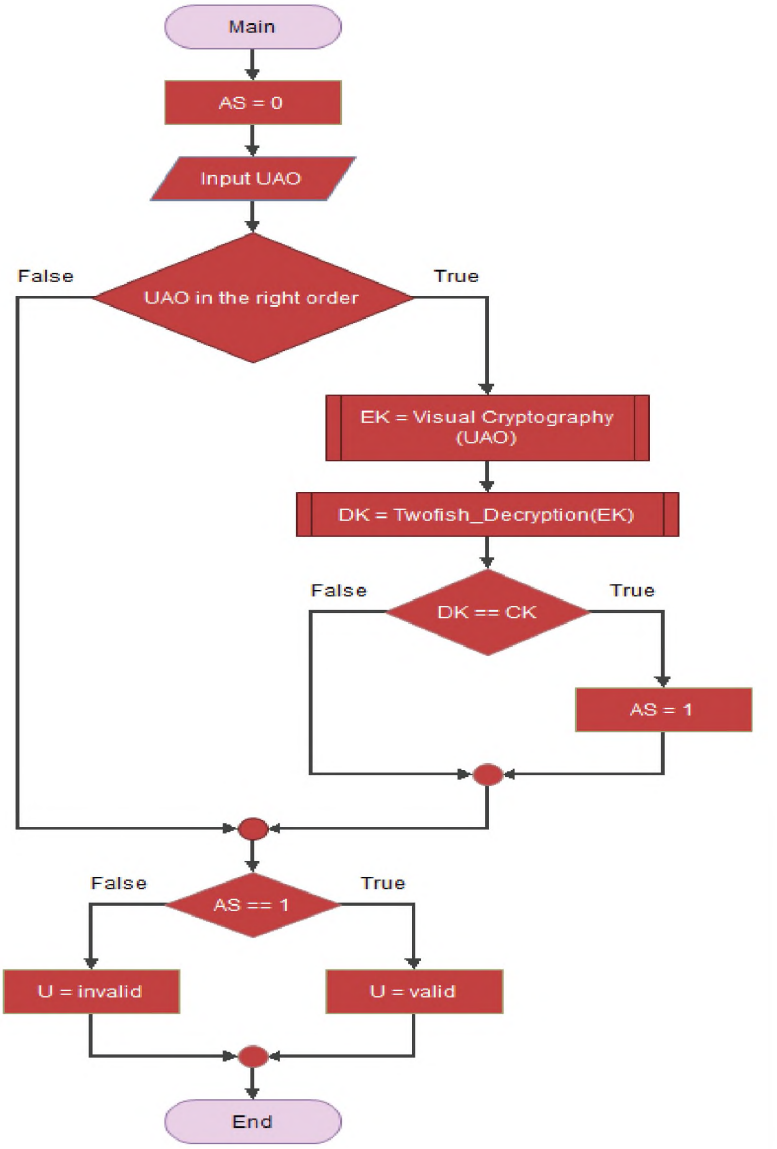

Figure 2 – showing authentication using TEVC

The keyword is entered:

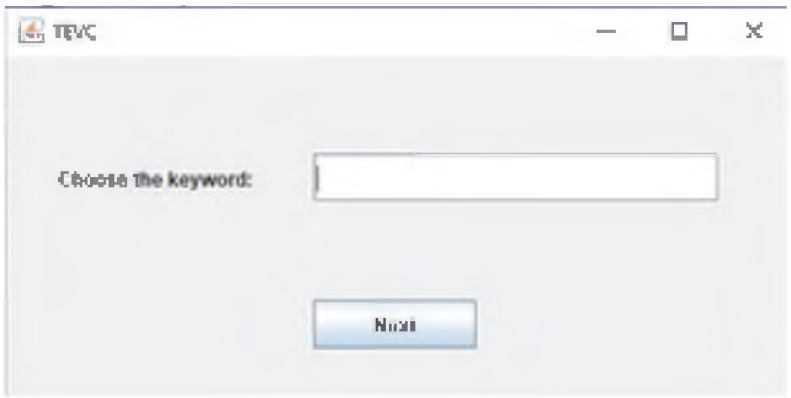

Figure 5 – keyword entering

Afterwards, the particles must be ordered by user's preference:

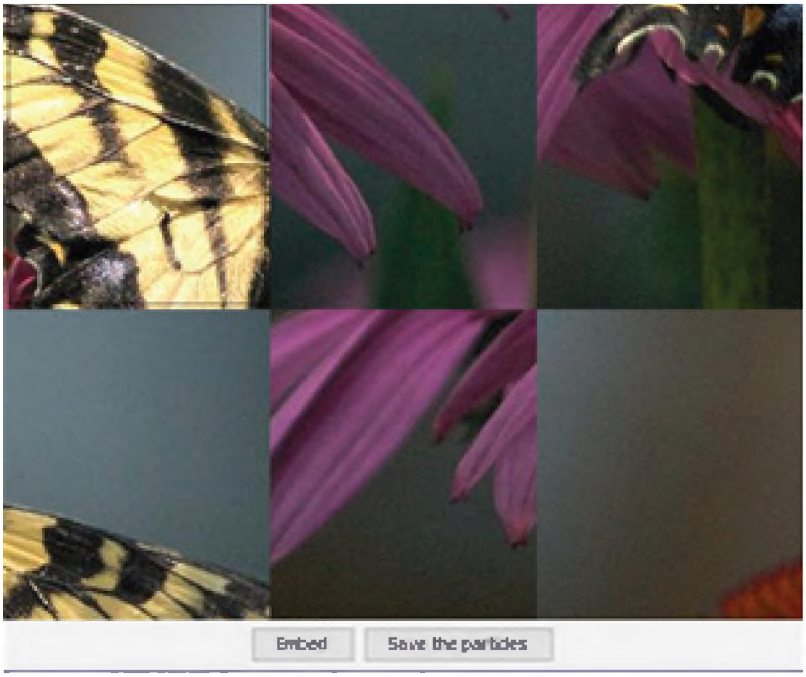

Figure 6 – ordering the particles

Furthermore, the encrypted keyword is embedded in the particles.

The system can be used in any field, where authentication is needed.

II. EXPERIMENTAL RESULTS

To conduct the experiments, the proposed TEVC algorithm is implemented on JAVA platform. The host operating system for java platform is Microsoft Windows-10. It runs on a computer with 8 Gigabytes of system memory, Intel® Core™ i3 processor and 2 terabytes of memory storage. Two experiments were performed. In the first experiment, reliability is measured. And in the second experiment, the time complexity is determined. The performance of proposed TEVC is measured and compared with contending algorithms: two-fish and visual cryptography. The similar parameters were used for proposed and contending algorithms. Based on the experimental result, we determined that proposed TEVC performed better than contending algorithms when using following metrics. Table 1 shows the experimental configuration.

- Reliability
- Time Complexity

A. Reliability

The reliability refers to the competency of the system to continuously achieve its required function on-demand and without decline or failure of the system. Figure 3 show the reliability of the TEVC algorithm and contending algorithms: Twofish and visual cryptography by using authentication process of maximum 450 users. In this experiment, 20% illegitimate users were also included. The reliability of the proposed TEVC algorithm is 100%, whereas other competing algorithms Twofish and visual cryptography have a reliability of 99.44% and 99.3% respectively. The results demonstrate that overall, the proposed TEVC algorithm is more reliable than other contending algorithms. The reliability is given by

Table 1: Configuration of Experimental Setup

Simulation Parameters	Configuration
Host Operating System	Microsoft Windows 10, 64 bit
Host Memory	8 Gigabytes DDR3
Programming Platform	Java
Hard Disk	2 terabytes
Host CPU	Intel® Core™ i3 processor 4160
Processing Speed	3.6 GHz (4logical cores per physical cores).
Host Model	Acer Aspire X

$$R = \frac{(I_s)}{(I_s - 1)}\left\{1 - \frac{(\sum P_i * A_i)}{(I_s - 1)}\right\} \qquad (11)$$

where

I_e is the total number of users, P_i is the authenticated users, A_i is the illegitimate users and $\sum$ is the sum.

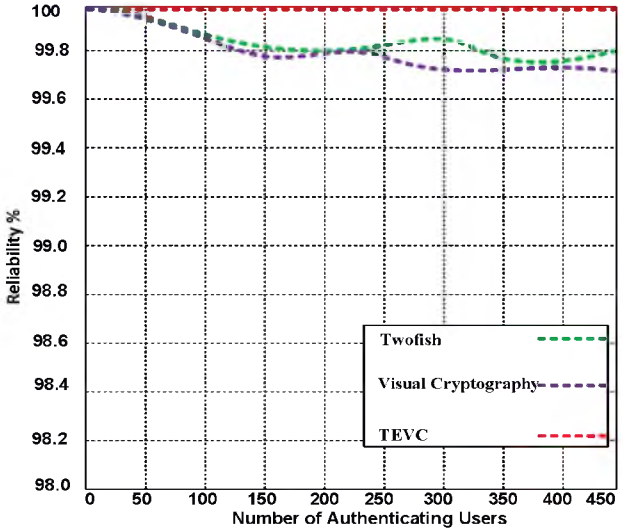

Figure 7 – Reliability of TEVC contending algorithms: Twofish and Visual cryptography

B. Time Complexity

The performance of algorithms depends on the less time complexity. The time complexity is the amount of time specified to perform as a task signifying the input. In Figure 4, we show the time complexity trend for TEVC, Twofish and visual cryptography algorithms. The results validates that proposed TEVC algorithm takes $O(n)$ time complexity, whereas visual cryptography and Twofish take (log n+ n) and $O(n\ log\ logn)$ respectively.

TEVC gives lowest time complexity as compared to other algorithms. The reason of having low latency is to use of features of twofish and visual cryptography. The time complexity of three algorithms is obtained using recursive approach given by equation 5.

$$T(n) = \{\ O(1)\ \ If\ \ n = 1$$

$$at\left(\frac{n}{b}\right) + O(n) If\ \ n > 1 \qquad (12)$$

Table 3: Time complexity for SDAAA and contending algorithms

Algorithms	Time complexity
TEVC	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ Problem consists of finite set of inputs, but its computation time linearly increases. Thus, $T(n) = t\left(\frac{n}{2}\right) + O(n)$ $T(n) = t + O(n)$ Where ignore t; therefore $T(n) = O(n)$
Twofish	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ Where problem is divided into two parts with same size. However, the algorithm is infinite. Thus. $T(n) = 2t\left(\frac{n}{2}\right) + O(n)$ $(n) = 4t\left(\frac{n}{4}\right) + n + n$ $T(n) = 4t + 2n$ $T(n) = O(kn)$ $T(n) = O(log\ lognn)$ Where k= log n $T(n) = O(n\ log\ logn)$
Visual Cryptography	$T(n) = at\left(\frac{n}{b}\right) + O(n)$ Problem consists of finite set of inputs, but computation complexity remains constant 'n' $T(n) = t\left(\frac{n}{2}\right) + O(n)$ $T(n) = t\left(\frac{n}{2}\right) + n + n$ $(n) = t\left(\frac{n}{n}\right) + n + n$ $T(n) = t(1) + n + n$ $T(n) = t + n + n$ Where ignore t; therefore, we get $T(n) = n + n$ Let n=k & k= log n T(n)= O(log n + n)

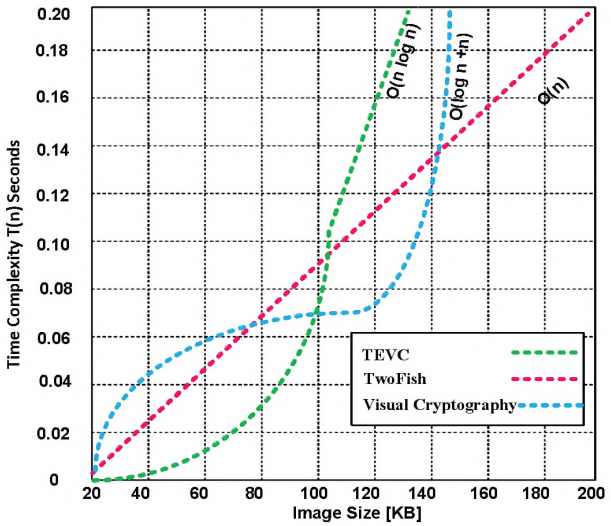

Figure 8 – Time complexity of TEVC, Twofish and visual cryptography

V. CONCLUSION

Improved graphical password authentication process using Twofish Encryption and Visual Cryptography method has been introduced. The proposed TEVC is randomly organized as predicting the correct graphical password and arranging its particles in the proper order. The proposed TEVC consists of user-adding to the system and authentication processes.

TEVC is tested by using JAVA programming. Based on the testing results, we confirm that proposed TEVC provides better reliability than contending algorithms: Twofish and visual cryptography. On the other hand, The TEVC encryption algorithm detected as more prudent and possessing lower time complexity as compared to contending algorithms. The TEVC produced 100% reliability that proves its strength.

REFERENCES

1. Yang, G., & Hwang, J. (2017). U.S. Patent No. 9,679,123. Washington, DC: U.S. Patent and Trademark Office.
2. Go, W., Lee, K., & Kwak, J. (2014). Construction of a secure two-factor user authentication system using fingerprint information and password. Journal of Intelligent Manufacturing, 25(2), 217-230.
3. Anwar, M., & Imran, A. (2015). A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In MAICS (pp. 13-18).
4. Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). Two-factor authentication: is the world ready?: quantifying 2FA adoption. In Proceedings of the eighth european workshop on system security (p. 4). ACM.
5. Erdem, E., &Sandıkkaya, M. T. (2019). OTPaaS—One Time Password as a Service. IEEE Transactions on Information Forensics and Security, 14(3), 743-756.
6. Persson, O., &Wermelin, E. (2017). A Theoretical Proposal of Two-Factor Authentication in Smartphones.
7. Raypure, R. M., &Keswani, V. (2017). Implementation For Data Hiding Using Visual Cryptography.
8. Chanda, K. (2016). Password security: an analysis of password strengths and vulnerabilities. International Journal of Computer Network and Information Security, 8(7), 23.
9. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Margolis, D. (2017, October). Data breaches, phishing, or malware?: Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 1421-1434). ACM.
10. Gualdoni, Joseph, et al. "Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication." Procedia computer science 114 (2017): 93-99.
11. Cherdmuangpak, Niramai, TanapatAnusas-amonkul, and BenchaphonLimthanmaphon. "Two factor image-based password authentication for junior high school students." 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE). IEEE, 2017.

12. Khandelwal, N. S., & Kamboj, P. (2015, January). Notice of Retraction Two factor authentication using Visual Cryptography and Digital Envelope in Kerberos. In 2015 International conference on electrical, electronics, signals, communication and optimization (EESCO) (pp. 1-6). IEEE.
13. Song, R. (2010). Advanced smart card based password authentication protocol. Computer Standards & Interfaces, 32(5-6), 321-325.
14. Zhao, H., & Li, X. (2007, May). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07) (Vol. 2, pp. 467-472). IEEE.
15. Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 37(11), 2245-2255.
16. Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish: A 128-bit block cipher. NIST AES Proposal, 15, 23.
17. Ibrahim, R., &Kuan, T. S. (2011). Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809.