A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme

IOP Conf. Series: Journal of Physics: Conf. Series **1299** (2019) 012059 doi:10.1088/1742-6596/1299/1/012059

A Secured One Time Password Authentication Technique using (3, 3) Visual Cryptography Scheme

Abikoye Oluwakemi Christiana[1], Akande Noah Oluwatobi[2*], Garuba Ayomide Victory[3], Ogundokun Roseline Oluwaseun[4]

[1,3]Computer Science Department, University of Ilorin, Kwara State, Nigeria
[2,4]Data and Information Security Research Group, Computer Science Department, Landmark University, Kwara State, Nigeria

*Corresponding Author: akande.noah@lmu.edu.ng

Abstract. The world is vastly becoming a completely digital one with most transactions carried out over the internet. This has exposed the internet to increasing threats and attacks and has necessitated the need for an internet-based authentication and authorization services. One Time Passwords (OTP) have been introduced to overcome the limitations of static passwords. However, research has shown that OTP are not completely free from middle man attacks. This paper presents a (3, 3) Visual Cryptographic Scheme (VCS) technique for OTP security. The technique secures the generated OTP image by dividing it into three shares, of which one of the shares will be sent to the user while the remaining shares will be stored at different locations on the server. Before the original OTP image will be recovered, all the shares must the retrieved and stacked together. To avoid pixel expansion problem and loss of image quality that have characterized existing VCS technique, progressive visual cryptography was adopted to decrypt the retrieved OTP shares. A high quality OTP image was recovered as revealed by the peak signal to noise ratio values and there was no change in size of the OTP images.

Keywords: Data Security, Information Security, One Time Password, Visual Cryptography Scheme, Progressive Visual Cryptography

1. Introduction

Sensitive data sent over a network needs to be securely kept from eavesdropping or attacks by intruders while the identity of an individual needs to be verified and authenticated before granting such access to the secured data/information. Existing authentication methodologies require the use of token, biometric and knowledge based techniques. Tokens entail the use of hardware such as smart cards or key cards while biometric technique entails the use of unique human traits such as voice, fingerprints, face, retina etc. Though effective, the major drawback of these approaches is their cost of implementation. Conversely, knowledge based authentication technique uses what a user knows such as a graphical or text based passwords. Graphical based passwords present the user with set of pictures or patterns that have been selected during the registration phase for authentication purposes. In contrast, text based passwords could be static or dynamic passwords; static passwords are mostly six or eight digit characters chosen by the user for authentication purposes. Both graphic and static passwords could be forgotten by the user, willingly divulged to a trusted person or accidentally

divulged under pressure. Similarly, they could be easily guessed by hackers which has made them prone to dictionary attacks as well as shoulder surfing [1,2]. These limitations led to the introduction of dynamic passwords aptly called One Time Passwords (OTP). They are system generated passwords that could only be used once and within a short period of time, therefore, providing a smaller window of time for an intruder to operate. According to authors in [3,4], OTP can be generated by synchronizing time between the server and the user, with the aid of random numbers or counters that increments after each use and through hash algorithms such as SHA-1 or MD-5.
After generation, OTP can be delivered to the appropriate individual through a proprietary token, an electronic mail or a Short Messaging Service (SMS). These media of OTP transmission have opened it up to several attacks [5,6,7]. Ten different OTP attacks such as: replay attack, forgery attack, impersonation attack, server impersonation attack, Denial-of-Service (DOS) attack, theft attack, hybrid theft attack, stolen verifier attack, theft DOS and server modification attack were identified by authors in [8]. Furthermore, eavesdropping through key logging, shoulder surfing, screen capturing are threats further identified in [9] while SMS phishing through the unconscious installation of malwares on users' phone is another possible threat identified in [10]. All these increasing threats have greatly undermined the security of data sent over a network and have necessitated the need to enhance their security. Visual Cryptography Scheme (VCS) has been extensively studied as a cryptographic technique for securing images. It was first proposed by Naor and Shamir in 1994 as a branch of cryptography that conceals information in images. Its principle of operation is clearly different from steganography which hides information in inconspicuous cover media [11]. Instead, VCS divides an image into n number of shares that are stored in 'n' different locations and any 's' shares are expected to be stacked together before the original image can be recovered [12, 13,14]. However, the original image could still be revealed by the human visual system without any knowledge of cryptography or encryption/decryption key [15].

2. Existing OTP Authentication Scheme Security Approaches

A two factor OTP authentication scheme was proposed by authors in [3]. One-way hash function was used to generate a hash chain OTP while another hash function was used to encrypt the OTP plaintext during transmission. During authentication, the current seed of the hash chain OTP retained by the server and the user were compared with the seeds of the entire hash chain on the server in order to ensure that the OTP submitted is authentic. Another attempt to secure OTP was proposed by authors in [16]. On receiving the OTP, the user is expected to generate a transaction password by supplying the OTP and the secret key into an offline mobile application which have been installed on user's mobile device. The mobile application was used to implement RSA algorithm in producing a transaction password from a passcode. The passcode is a combination of the generated OTP and a secret key known to the user alone. To generate the passcode, the summation of the digits of the secret key was inserted into the OTP at a position specified by the last digit of the OTP. Similarly, authors in [4] proposed a multi-channel approach to securing OTP. RC4-EA encryption technique was used to encrypt the OTP while Quick Response (QR) code was used to hide the encrypted OTP. For the authentication purpose, the user is expected to upload the QR-OTP sent to the email as well as the OTP sent to the Phone. The proposed multi-channel authentication approach was expected to guarantee the security of the OTP against eavesdropping. Furthermore, the possibility of integrating features extracted from biometric traits and cryptography to enhance OTP security have been reported. Authors in [17] employed Elliptic Curve Cryptography (ECC) and fingerprint to enhance OTP security. ECC was used to encrypt the generated OTP before sending it over a network while MD5 cryptographic hash function was used to compute the secret keys from the extracted fingerprint features. Similarly, features extracted from iris with ECC towards achieving a secured OTP transmission was proposed in [18]. The encryption and decryption time recorded revealed that a faster encryption time but a slower decryption time was achieved when ECC alone was used. In the same way, authors in [7] used features extracted from users' voice samples and ECC to achieve a two-way

authentication technique. However, a faster encryption time and a slower decryption time was achieved. On the contrary, an OTP authentication scheme using Negative Database (NDB) was proposed in [19]. The generated OTP was converted to a NDB before sending it over the network. The authors leveraged on the fact that reversing a NDB in order to retrieve its content is a NP-Hard problem, therefore, even if an attacker intercepts the NDB the OTP cannot be recovered.

3. Existing OTP Authentication Scheme Security Approaches

Furthermore, VCS technique has also been extensively used to secure images carrying confidential information. Such is seen in a challenge-response visual cryptography OTP authentication scheme that works with a mobile device's camera; this was proposed in [5]. In addition to securing the OTP, the proposed approach also introduces an OTP authentication scheme that is not SMS based therefore not reliant on mobile phone network reception. Users are first expected to register the International Mobile Station Equipment Identity (IMEI) of their mobile device on the authentication server after which the visual OTP software will be downloaded. The OTP shares are in form of QR code and users are expected to scan the first QR code share and overlay it on the second QR code before the OTP will be revealed. The distinctiveness beauty of the proposed technique is that only the user's registered mobile device can be used to correctly scan the QR code, also, the user's mobile device will be responsible for scaling and aligning the patterns. However, the proposed scheme does not cater for man-in-the- middle attack and also does not make provision for instances where the authentication server is hacked. Anadditional layer of security was introduced to (2, 2) XOR based VCS in [15]. After generating the shares, Advanced Encryption Standard (AES) algorithm was used to further encrypt each share before sending them over the network. Though the encryption and decryption of the shares with AES increased the total computation time, an encryption and decryption time of 0.095 and 0.011 seconds were reported. Similarly, a QR based (2, 3) and (3, 3) Extended Visual Cryptography Technique (EVCT) was proposed for sharing coloured images in [14]. Meaningful shares were generated in the proposed technique using the RGB components of the image. No data was lost during the decryption process and the recovered secret image had a good contrast. A total execution time of 3s and 5s were recorded for (3, 3) EVCT and (2, 3)–EVCT respectively. Furthermore, a VCS that divides an original image into four shares was proposed in [13]. Instances where two, three and four of the shares were XORed together in order to reveal the original image were reported. The visual quality of the recovered image to the original image was measured using Peak Signal-to-Noise Ratio (PSNR). Result obtained revealed that the best image quality was achieved when all the four shares were superimposed together. This article is aimed at further enhancing the security of OTP using (3,3) Visual Cryptographic Scheme. Firstly, an OTP image was created using Time-Based One Time Password (TOTP) generation technique. Afterwards, three different shares were generated from the created OTP image; all the shares must be stacked together in order to retrieve the original OTP image. To control pixel expansion problem and also to ensure the retrieval of a high quality OTP image, Progressive Visual Cryptography (PVC) was employed to stack the shares in a progressive manner.

.

4. Materials and Methods

The proposed VCS based OTP authentication scheme consists of three phases: OTP generation, OTP encryption using (3,3) VCC and OTP decryption using PVC.

4.1. OTP Generation Technique

A keyed-hash message authentication code (HMAC) OTP (HOTP) generation technique proposed in [20] was adopted for OTP generation. This is a synchronous method of OTP generation that uses an

increasing counter value and a static symmetric secret key. HMAC-SHA-1 algorithm as defined in RFC 2104 was employed to generate an HOTP value. However, the 160 bits (20 bytes) output of the HMAC-SHA-1 algorithm was truncated to 32 bits (4 bytes) so that it can be easily entered by any user. Thus, the HOTP generation algorithm can be summarized as:

Step i: Compute the time difference (T) between the initial counter time and the current system time.

Step ii: Generate a HMAC-SHA-1 value such that:

HS = HMAC-SHA-1(K, T)

Note that the resulting HS is a 20byte string.

Step iii: Using Dynamic Truncation (DT), generate a 4-byte string from the value of HS in step ii such that:

Step a: S = DT (HS)

where S is the 4-byte value

HS = String [0] ...String [19]

Step b: Let offset bits Offset be the low-order 4 bits of String [19] such that:

Offset = StToNum(OffsetBits)

where 0 <= OffSet <= 15

Step c: Let P = String [OffSet]...String[OffSet+3]

Step d: Return the last 31 bits of P (the truncated 4 bytes)

Step iv: Compute a TOTP value using the following steps:

Step a: Let Snum = StToNum(S)

This converts S to a number in 0...2^ {31} -1

Step b: Return D = Snum mod 10^Digit

where D is a number in the range 0...10^{Digit}-1

4.2. OTP Encryption and Decryption using (3,3) VCS and PVC Technique

The traditional VCS was adjusted to generate a codebook such that a matrix C_0 is obtained by permuting the columns of $\begin{matrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ ... & ... & ... & ... \\ 1 & 0 & 0 & 0 \end{matrix}$ and a matrix C_1 is obtained by permuting the columns of $\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ ... & ... & ... & ... \\ 0 & 0 & 0 & 1 \end{matrix}$.

C_0 is used to generate shares for white pixels of the image while C_1 is used for black pixels. The final basis matrix used are:

$$C_0 = \begin{matrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \quad \text{and } C_1 = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}$$

Based on the generated codebook, the OTP image was encrypted using the following steps:

a) Select a pixel from the input OTP image
b) Determine if the pixel is black or white
   If white:
   i. Select a block randomly from the three blocks of the white pixel in the codebook.
   ii. Choose a row to be assigned to vector V from the block
   If black:
   i. Select a block randomly from the three blocks of the black pixel in the codebook.
   ii. Choose a row to be assigned to vector V from the block
c) Construct 3 shares s1, s2 and s3from vector V.
d) Repeat a) to c) and stop when all the pixels have been shared.

To prevent OTP image size expansion and quality distortion during the decryption process, the encrypted OTP image shares were decrypted by progressively stacking the shares together using XOR operation such that:

i. each image share was randomly selected from shares s1, s2 and s3
ii. the recovered secret image R was obtained using XOR operation such that R = s1⊕ s2 ⊕ s3 or s1⊕ s3 ⊕ s2 or s2⊕ s1 ⊕ s3 or s2⊕ s3 ⊕ s1 or s3⊕ s1 ⊕ s2 or s3⊕ s2 ⊕ s1.

Flowchart shown in Fig. 1 highlights the whole process of OTP generation, encryption and decryption which were encapsulated into a web application. The results obtained are discussed in details in the next section.

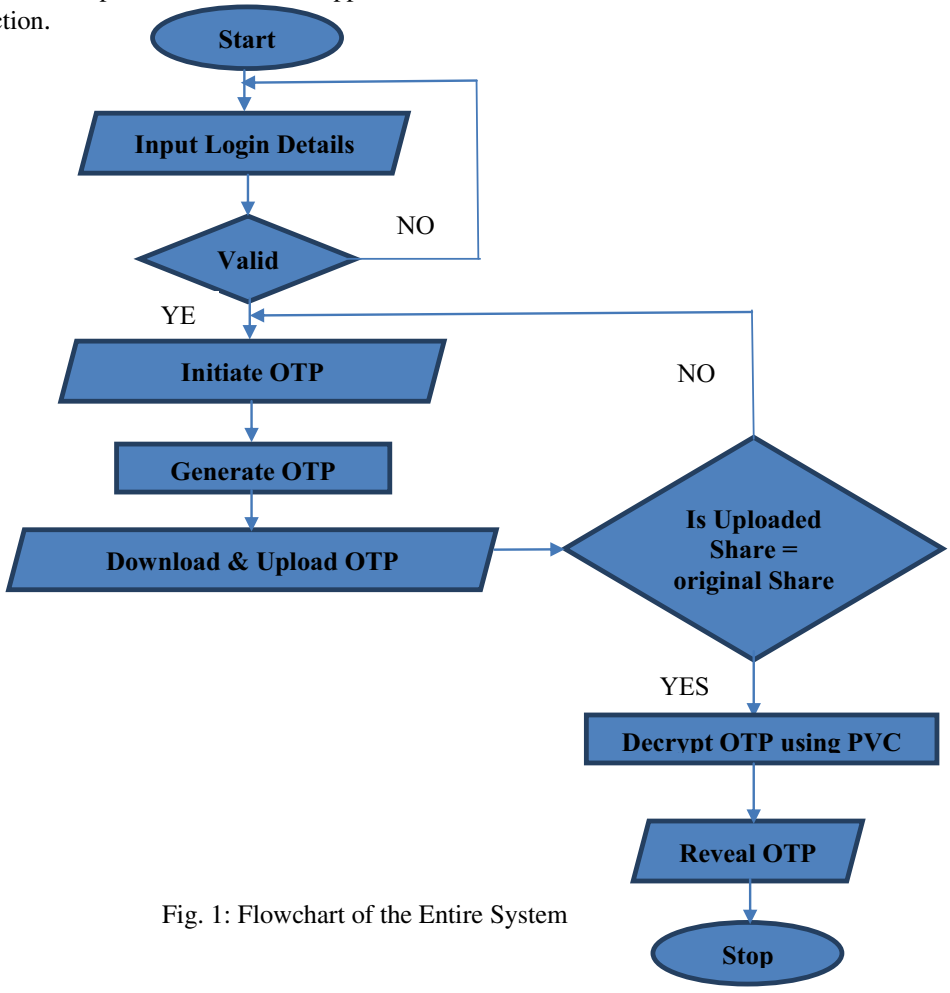
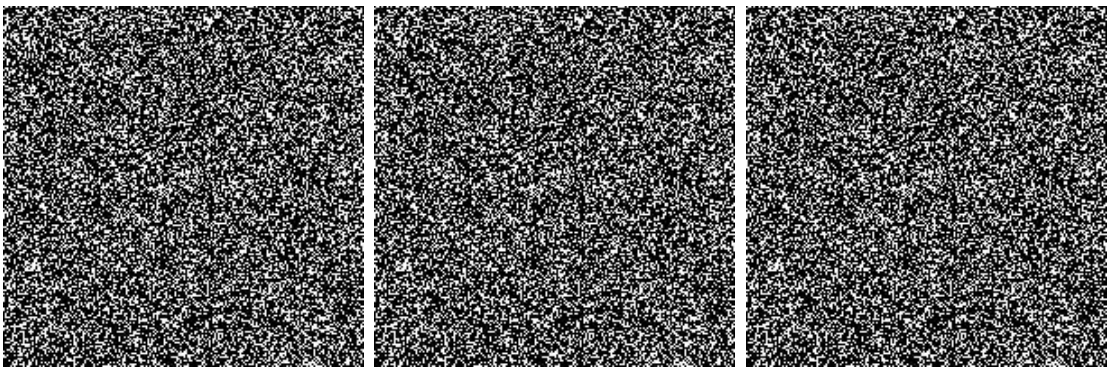


Fig. 1: Flowchart of the Entire System

5. Results and Discussion

HOTP generation technique was used to produce the OTP image as shown in Fig. 2. However, the generated OTP will not be displayed to users as it was encrypted using (3,3) VCS. The generated OTP image was divided into 3 shares as shown in Fig. 3a-3c. One of these shares will be made available to the user while the remaining shares will be stored at different locations on the server.

Fig. 2: OTP Image Generated



a) Encrypted Share 1 b) Encrypted Share 2 c) Encrypted Share 3

Fig. 3: Encrypted Shares using (3,3) VCS Technique

As illustrated in Fig. 4, users are expected to download an OTP share which is one of the encrypted shares shown in Fig. 3. Afterwards, the downloaded share is expected to be uploaded using the web interface shown in Fig. 5.

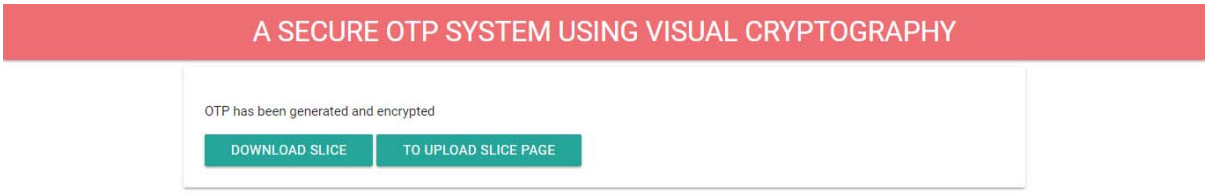


Fig. 4: OTP Slice Download Interface

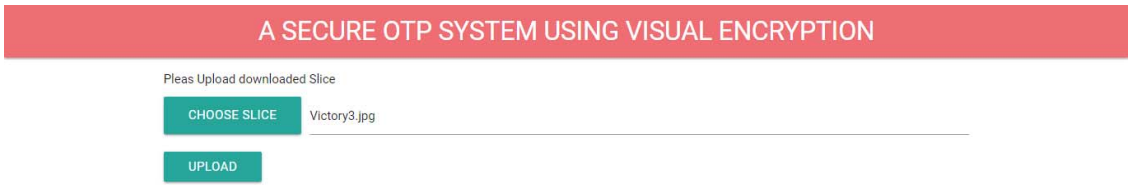
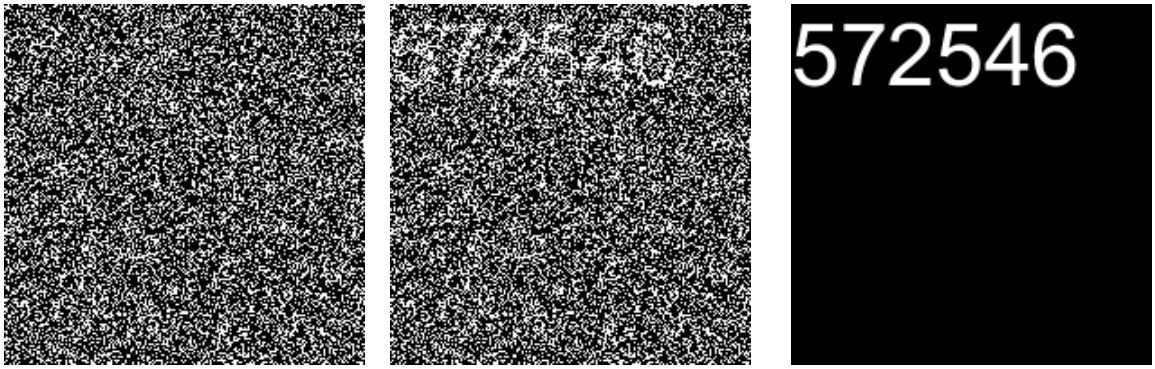


Fig. 5: OTP Slice Upload Interface

The uploaded OTP share is compared with the original share sent to the user, if valid, other shares are fetched and stacked progressively using PVC technique before the final OTP image is revealed. Fig. 6 presents the OTP images generated when the shares are stacked progressively using PVC technique.



a) Share 1 b) Share 1 XOR Share 2 c) Share 1 XOR Share 2 XOR Share 3

Fig. 6: Decrypted Shares using PVC Technique.

Finally, the decrypted OTP image is displayed to the user as shown in Fig. 7.

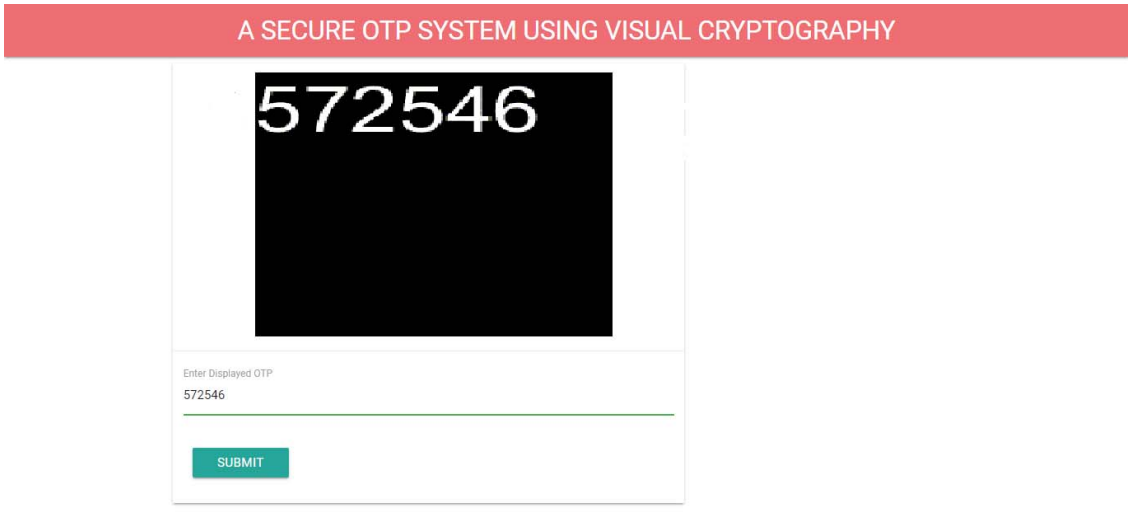


Fig. 7: Decrypted Share Displayed to the User

5.1. Performance Evaluation

The recovered OTP images have the same size as the original OTP images; this affirms that there was no pixel expansion during the OTP image encryption and decryption process. Furthermore, Peak Signal to Noise Ratio (PSNR) which is a function of the Mean Squared Error (MSE) was used to measure the change in quality between the recovered OTP image and the original OTP image. This was carried out to determine if there was loss in image quality during the encryption and decryption process. The MSE was computed using equation 1 while the PSNR was calculated using equation 2 such that:

$$MSE = \frac{1}{M\ x\ N}\sum_{i=1}^{M}\sum_{j=1}^{N} O_{ij} - R_{ij} \quad (1)$$

$$PSNR = 10log\frac{Max^{2}}{MSE} \quad (2)$$

Where O_{ij} is the original OTP image with pixels i and j while R is the recovered OTP image pixels i and j. Max is the highest possible pixel value of the images while M and N are the maximum pixel value of the original and recovered OTP image respectively. Using different combinations of shares to recover the OTP image, the PSNR values computed are provided in Table 1.

Table 1: Computed PSNR Values

S/N	STACKED SHARES	PSNR VALUE (db)
1.	Share 1 XOR Share 2 XOR Share 3	33.39
2.	Share 1 XOR Share 3 XOR Share 2	32.95
3.	Share 2 XOR Share 1 XOR Share 3	33.75
4.	Share 2 XOR Share 3 XOR Share 1	33.86
5.	Share 3 XOR Share 2 XOR Share 1	33.42
6.	Share 3 XOR Share 1 XOR Share 2	33.40

6. Conclusion

This article emphasizes the need to further secure OTP from several attacks. It highlighted several approaches that have been used in the literature and also explored the prospect of using (3,3) VCS technique. HOTP generation technique was used to create the OTP before dividing the OTP image into three shares. One of the shares is the user's share while the remaining shares are stored in a secured place on the server. To recover the original OTP images, all the shares were stacked together in a progressive manner using PVC; this is to prevent pixel expansion problem which has characterized existing VCS techniques. PSNR values computed from the original as well as the recovered OTP images revealed that the recovered OTP images were of high quality and does not suffer pixel expansion. Therefore, the technique employed can be used to secure OTP images.

Acknowledgement

Authors appreciate Landmark University Centre for Research and Development, Landmark University, Omu-Aran, Nigeria for fully sponsoring the publication of this article.

References

[1]. Sanket Prabhu & Vaibhav Shah (2015). Authentication using session based passwords. Procedia Computer Science, 45, 460-464.
[2]. Abikoye Oluwakemi Christiana, Haruna Ahmad Dokoro, Akande Noah Oluwatobi (2019), "Modified Advanced Encryption Standard Algorithm for Information Security", Journal of Applied Science and Engineering, Vol. 22, No. 2.
[3]. Huiyi Liu & Yuegong Zhang (2013), "An Improved One-time Password Authentication Scheme. In Proceedings of 15th IEEE International Conference on Communication Technology, 1-5.
[4]. Ashraf Aboshosha, Kamal A. El-Dahshan, Eman K. Elsayed & Ahmed A. Elngar (2015). Multi-channel user authentication protocol based on encrypted hidden OTP. International Journal of Computer Science and Information Security, 13(6), 14-19.
[5]. Chow Yang-Wai, Susilo Willy, Au Man Ho & Barmawi Ari Moesriami (2015). A visual one-time password authentication scheme using mobile devices., In L. C. K. Hui, S. H. Qing, Shi E & Yiu S. M. (2014), Proceedings of the 16th International Conference on Information and Communications Security (ICICS 2014), 243-257. Switzerland: Springer International Publishing.
[6]. Thomas M. & Panchami V. (2015). An encryption protocol for end-to-end secure transmission of SMS. International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], 1–6
[7]. Komal K. Kumbhare & Warkar K. V. (2016). A review on noisy password, voiceprint and One-Time Password. Procedia Computer Science, 78, 382-386.
[8]. Ryoichi Isawa & Masakatu Morii (2011). One-Time Password Authentication Scheme to Solve Stolen Verifier Problem. Information Processing Society of Japan and The Institute of Electronics, Information and Communication Engineers, 225-228.
[9]. Ariel Roy L. Reyes, Enrique D. Festijo & Ruji P. Medina (2018). Securing one-time password (OTP) for multi-factor out-of-band authentication through a 128-bit Blowfish Algorithm International Journal of Communication Networks and Information Security, 10(1), 242-247
[10]. Collin Mulliner, Ravishankar Borgaonkar, Patrick Stewin & Jean-Pierre Seifert (2013). SMS-based one-time passwords: Attacks and defense. In K. Rieck, P. Stewin, and J.-P. Seifert, editors, DIMVA, volume 7967 of Lecture Notes in Computer Science. 150-159. Springer Publishers.
[11]. Priyanka Singh & Balasubramanian Raman (2018). Reversible data hiding based on Shamir's secret sharing for color images over cloud. Information Sciences, 422, 77–97.
[12]. Pei-Ling Chiu & Kai-Hui Lee (2015), "User-friendly threshold visual cryptography with complementary cover images", Signal Processing, 108, 476–488
[13]. Mahmoud E. Hodeish, Linas Bukauskas & Vikas T. Humbe (2016). An Optimal (k, n) Visual Secret Sharing Scheme for Information Security. Procedia Computer Science, 93, 760 – 767
[14]. Dhiman K.& Kasana S. (2017). Extended visual cryptography techniques for true color images., Computers and Electrical Engineering, 1-12
[15]. Shankar K & Eswaran P (2015). Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. Procedia Computer Science, 70, 462 – 468.

[16]. Safa Hamdare, Varsha Nagpurkar & Jayashri Mittal (2014). Securing SMS Based One Time Password Technique from Man in the Middle Attack. International Journal of Engineering Trends and Technology, 11(3), 154–158.

[17]. Dindayal Mahto & Dilip Kumar Yadav (2015). Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Finger-Print Biometric. Proceedings of the 2nd International Conference on Computing for Sustainable Global Development, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA), 301-306

[18]. Dindayal Mahto & Dilip Kumar Yadav (2016). Security Improvement of One-Time Password Using Crypto-Biometric Model. Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Smart Innovation, Systems and Technologies, Springer India, 347-353

[19]. Dongdong Zhao & Wenjian Luoa (2017). One-time password authentication scheme based on the negative database. Engineering Applications of Artificial Intelligence, 62, 396-404

[20]. M'Raihi D., Bellare M., Hoornaert F., & Naccache D. (2005), "HOTP: An HMAC based one-time password algorithm. Http://tools.ietf.org/html/rfc4226.txt