Secure One-Time Password Generation Using Shamir's Secret Sharing

Naman Aggarwal[1], Sonam Kumari[2], Sanya Bahl[3], Uday Jain[4], Nitasha Rathore[5], Dharmender Saini[6]

Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi

Abstract

The process of authenticating users is critical for ensuring security. Static passwords are a popular and traditional authentication method due to their simplicity, but they are vulnerable to attacks such as password leakage, replay, guessing, eavesdropping, phishing, and spoofing, among others. One-time passwords (OTP) were introduced to address these limitations, but research has found that they are not immune to middle man attacks. To enhance the security of OTP, a new technique called Visual Cryptography Schema is proposed in this paper. In this method, we use Shamir's Secret Sharing theory in which the main OTP is parted into three shares. Out of these shares, one is sent to the user and the other two shares are stored in different locations in the server. To retrieve the original OTP, one must combine all the three shares.

Keywords: Cryptography, One Time Password (OTP), Eavesdropping, Visual Cryptography Scheme, Middle man attack, Shamir's Secret Sharing, Data Security, Three-share distribution

I. INTRODUCTION

The protection of sensitive information transmitted over a network is critical in preventing eavesdropping and intrusion, and it is essential to confirm and validate the identity of anyone seeking ingress to the protected information. Validation methods such as tokens, biometrics, and knowledge-based techniques are utilized in current methodologies. However, the high implementation costs associated with these methods are a significant drawback. Knowledge-based authentication techniques employ a user's knowledge. Graphical-based passwords involve a collection of images or patterns chosen throughout the verification registration procedure, while static text-based passwords typically consist of six or eight-digit characters selected by the user. However, both static and graphical passwords can be forgotten, revealed deliberately or unintentionally. To address these issues, dynamic passwords known as One Time Passwords (OTP) were introduced. After generation, OTP can be sent to the intended recipient through various transmission media, including a proprietary token, email, or SMS. However, these transmission mediums have made OTP vulnerable to numerous attacks such as replay, forgery, and impersonation attacks, among others. Threats related to eavesdropping by key logging, shoulder surfing, and screen capture are also a concern.To improve the security of data transmitted, deep research has been done on Visual Cryptography Scheme (VCS) as potential way of cryptographically protecting images.

VCS is a subset of cryptography that conceals data within images and was first proposed by Naor and Shamir in 1994. Unlike steganography, which hides information under cover material that is not readily visible, VCS separates an image into n shares that are kept in n various places, and any s shares that cannot be placed together must be stacked together before the initial picture can be restored. The human visual system can decrypt the original image without the use of encryption or decryption keys.

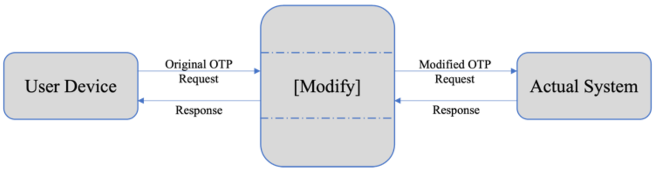


Figure 1 – Men in the middle System

The protection of sensitive information transmitted over a network is crucial in preventing eavesdropping and intrusion. Authentication techniques such as tokens, biometrics, and knowledge-based methods are used to authenticate users, but the high implementation costs associated with biometric techniques are a significant drawback. The use of graphical and text-based passwords can also pose security risks, and dynamic passwords such as OTP are not immune to attacks. A potential cryptographic technique for safeguarding images is the Visual Cryptography Scheme (VCS), which has undergone extensive research. It divides images into shares stored in distinct locations and can be decrypted without encryption or decryption keys by the human visual system.

II. RELATED WORK

A paper discussing cryptography by Abdal Basit Mohammed Qadir and Nurhayat Varol presented a survey of research conducted on topics such as Transposition ciphers, Modern algorithms (Stream ciphers, Block ciphers), Hash functions, and public key systems. The paper also explained the workings of various algorithms used in cryptography for different security goals [16]. The authors predicted that cryptography would continue to play a crucial role in IT and business planning to protect personal, financial, medical, and ecommerce data while preserving the privacy and availability of users. Thomas M. and Panchami V. presented an efficient encryption protocol that allows secure transmission of confidential SMS messages between mobile users. The protocol satisfies cryptographic goals such as confidentiality, authentication, and message integrity [6]. The research study employs the EasySMS protocol for authentication and the Blowfish encryption technique for confidentiality.

The review article titled "Cryptography: A Comprehensive Overview" by Qadir and Varol [16] provided an overview of research in cryptography, including transposition ciphers, modern algorithms such as stream and block ciphers, hash functions, and public key systems, as well as the functionality of these algorithms for different security goals. The authors predicted that cryptography would continue to play a key role in protecting personal, financial, medical, and ecommerce data while maintaining user privacy and availability.

In their paper, Thomas, and Panchami [6] propose an efficient encryption protocol for secure transmission of confidential SMS messages between mobile users, which achieves confidentiality, authentication, and integrity. The Blowfish encryption algorithm provides confidentiality, the EasySMS protocol provides authentication, and the MD5 hashing algorithm ensures integrity of the messages. The authors also claim that the Blowfish algorithm consumes less battery power than other encryption algorithms, and their protocol prevents various attacks, including SMS disclosure, replay attacks, man-in-the-middle attacks, and over-the-air modification.

A protocol for multi-channel user authentication based on encrypted hidden OTP was presented by Aboshosha, El-Dahshan, Elsayed, and Elngar in their paper [4]. The proposed protocol uses RC4-EA encryption to encrypt plain-OTP into cipher-OTP, which is then hidden in a Quick Response (QR) code. The protocol aims to integrate web-based and mobile-based technologies for multi-channel authentication, and its main advantage is to secure the authentication system against eavesdropping attacks. The authors claim that their proposed protocol overcomes several challenging attacks, such as replay attacks, DoS attacks, man-in-the-middle attacks, and real-time phishing attacks.

Using a 3x3 Vedic multiplier, Shyry and Mahithaasree [19] present a mechanism for producing OTP. Both the communication's duration and the recipient's login information from the Certificate Authority are transformed to 8 bits. To create the OTP, these 16 bits are translated to decimal using CB2D, and two sets of three decimal numbers are multiplied by a 3x3 Vedic exponent. However, because it needs to be aware of the user's credentials, which an attacker may gain to produce OTP, this method is not protected.

The paper by Isawa and Morii [8] presents a new one-time password scheme that addresses the Hybrid Theft attack. The proposed scheme has three advantages: it is secure against existing attacks, based on only one-way hash function, and a mutual authentication scheme. The authors claim that their proposed scheme is more secure and faster than the SAS-X (2) one-way authentication scheme. In their research paper titled "Addressing Challenges in Achieving Human-Friendly Encryption," Kimmo Halunen and Outi-Marja Latvala [21] outlined several concerns and obstacles that must be resolved to create encryption methods that are easy for humans to use.

In "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks" [20], Paula Fraga-Lamas and Tiago M. Fernández-Caramés presented a comprehensive overview of current quantum blockchain security and potential future developments. They examined the most promising post-quantum public-key encryption and signature systems while analysing the effects of quantum-processing assaults on blockchain.

Dongdong Zhao and Wenjian Luo developed a one-time password (OTP) generation method using Negative Database (NDB) [3]. Their approach involved concatenating a random seed with the user password, hashing the result to create the Database (DB), and then using the same seed to compute the NDB. In their paper "Extended Techniques for Visual Cryptography of True Color Images" [14], Dhiman K. and Kasana S proposed two extended visual cryptography techniques for sharing color images that are less complex and lossless in nature. The proposed techniques involve generating three meaningful shares using a block size of 5 × 5 corresponding to each pixel of the original secret image.

Yuji Suga proposed a novel one-time password generation model that combines the hash chain using Merkle tree and L-divided tree and referred to it as the "Sausage-style" one-time password [1,4]. However, no implementation has been conducted for this model yet. Suga also provided further clarification for his proposed model by giving more examples, but it remains untested due to the lack of implementation. [5]

III. EXISTING OTP AUTHENTICATION SCHEME SECURITY APPROACHES

The protection of sensitive information during transmission over a network is of utmost importance to prevent unauthorized access. Therefore, various methods of user authentication are implemented to confirm the identity of individuals seeking access to protected data. However, these methods often come with their own set of risks and limitations, making it imperative to continuously improve network security. To ensure secure OTP authentication, the authors of [3] suggested a two-factor technique. This method involved the encryption of OTP plaintext using a different hash function during transmission. In [15], another approach to securing OTP was proposed, which involved the use of an offline mobile application downloaded to the user's mobile device. The user was required to enter the OTP and secret key into the application to create a transaction password.

The authors of [4] proposed the use of multiple channels to secure OTP, which involved encrypting the OTP using the RC4-EA encryption algorithm. Both the OTP and QR-OTP were uploaded to the user's phone and email for authentication purposes. Application of a multi-channel authentication mechanism helped to combat eavesdropping of OTP. In addition, biometric attributes and cryptography can be used to enhance OTP security. In [17], fingerprint and Elliptic Curve Cryptography (ECC) were utilized to increase OTP security. The OTP was encrypted using ECC and secret keys were generated using extracted fingerprint features and the MD5 cryptographic hash function. The authors of [18] suggested a secured OTP transmission using characteristics derived from the iris and ECC. However, it was revealed that with ECC the process of encryption was faster but the process of decryption was much slower. Similarly, in [7], a two-way authentication method was developed using user voice samples and ECC, although it led to a faster encrypting time and slower decryption time.

In contrast, a Negative Database (NDB)-based OTP authentication mechanism was suggested in [19]. Before transferring the OTP over the network, an NDB was created from it. The authors made use of the fact that it is NP-Hard to reverse an NDB and obtain its content, which implies that even if an attacker intercepts the NDB, the OTP cannot be retrieved. Protecting sensitive information transmitted over a network from eavesdropping and intrusion is critical. OTP authentication methods are implemented to verify the identity of individuals requesting access to protected data, but their limitations and associated risks necessitate continuous improvement. Various approaches involving multiple channels, biometric attributes, and cryptography have been suggested to enhance OTP security. The implementation of these measures will help ensure the safety and confidentiality of sensitive information transmitted over a network.

IV. VISUAL CRYPTOGRAPHY SCHEMA

One cryptographic technique that can be used to encrypt visual information, such as images and text, is known as visual cryptography. This technique results in the production of a visual image when the information is decrypted. In 1994, Naor and Shamir introduced a secret sharing method where an image is split into n shares and at least n-1 shares are needed to decrypt it. In this method, for each pixel in the original image, two pixels are present in each component image. If the original pixel was black, the pixel pairs in the component images must be complimentary, resulting in a dark grey color when overlapped. Conversely, if the original pixel was white, the pixel pairs in the component images must match, resulting in a light grey color when overlapped.

In order to create encryption schemes, specific pixel patterns are needed to encrypt black and white images using their pixels. For white pixels, a randomly chosen pattern (such as horizontal, vertical, and diagonal) is used for each image. If two images both have white pixels encrypted using the same pattern, their combination will yield the same result as that present in the pattern.

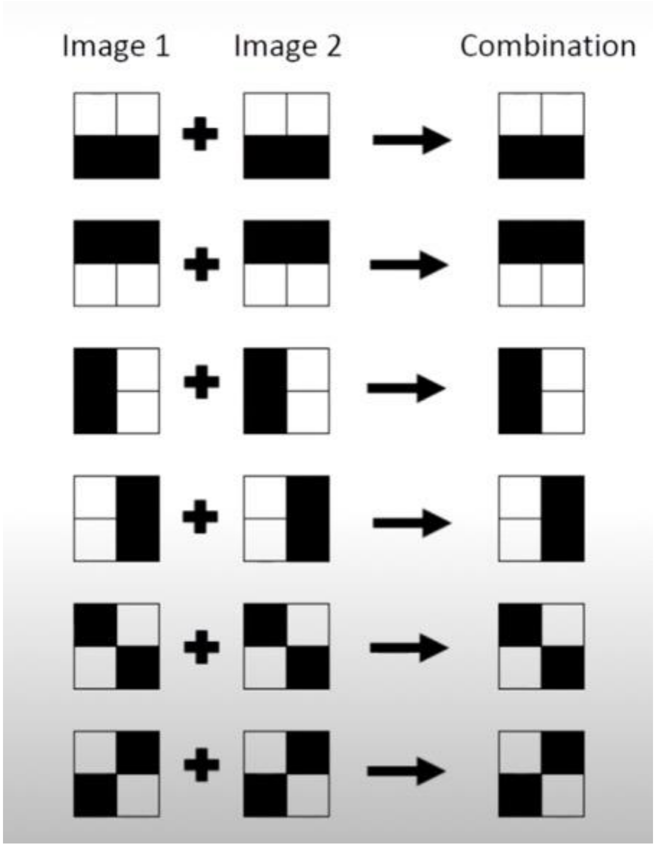


Figure 3 – White pixel encryption in VCS

In order to encrypt black pixels, a random pattern (horizontal, vertical, or diagonal) and its inverse are selected for each image. Similarly, when a black pixel is encrypted in two images, the resulting pattern will be black.

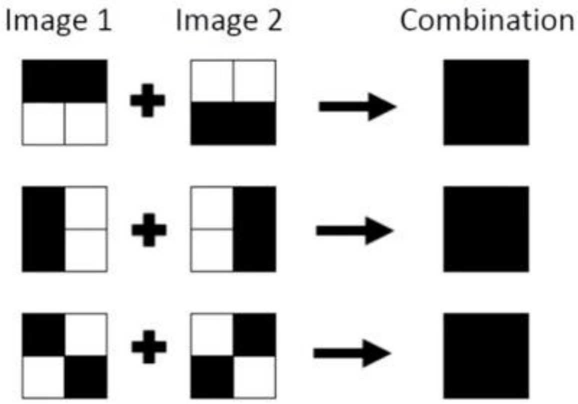


Figure 3 – Black pixel encryption in VCS

V. PROPOSED METHODOLOGIES

The method that we have proposed in this paper is a three-phase scheme that includes OTP generation. This scheme aims to provide secure and user-friendly authentication for online services. The OTP generation technique used in this scheme is a keyed-hash message authentication code (HMAC) OTP

(HOTP) generation method as suggested in [20]. This method employs a static symmetric secret key and a growing counter value for synchronous OTP generation. The HMAC-SHA-1 algorithm was used to create an HOTP value. This algorithm is described in RFC 2104 and is commonly used for message authentication. The HMAC-SHA-1 technique involves computing a hash value by applying a secret key to a message and appending the resulting hash to the original message. To reduce the complexity of entering the OTP for the user, the output of the HMAC-SHA-1 algorithm was reduced from 160 bits (20 bytes) to 32 bits (4 bytes).

The use of a symmetric secret key ensures that only the user and the server can generate and validate the OTP. The growing counter value ensures that each OTP is unique and cannot be reused. The use of HMAC-SHA-1 ensures the integrity and authenticity of the OTP, as any tampering with the OTP or the secret key will result in an invalid HMAC. The OTP encryption phase of the scheme involves the use of a (3,3) VCC. A VCC is a visual cryptography scheme that involves splitting a secret image into multiple shares such that the secret can only be revealed when the shares are superimposed. In this scheme, the OTP is split into three shares using a (3,3) VCC. The decryption phase of the scheme involves the use of a PVC. A PVC is a visual cryptography scheme that involves overlaying multiple shares to reveal the secret image. In this scheme, the three shares of the OTP generated in the encryption phase are superimposed using a PVC to reveal the original OTP.

Overall, the proposed VCS based OTP authentication scheme provides a secure and user-friendly authentication mechanism for online services. The use of HMAC-SHA-1 for OTP generation ensures the integrity and authenticity of the OTP, while the use of VCC and PVC schemes ensures the confidentiality of the OTP during transmission. The growing counter value ensures the uniqueness of each OTP, preventing replay attacks. The proposed algorithm for generating one-time passwords (OTPs) involves three main steps: OTP generation, OTP encryption, and OTP decryption. To generate the OTP, a synchronous technique called HMAC OTP (HOTP) generation was used. This technique requires a static symmetric secret key and a counter value that increases over time. The time difference (T) between the original counter time and the current system time must first be calculated in order to produce the HOTP. Next, T and the secret key are used to create an HMAC-SHA-1 value. The resulting 20-byte string is the HMAC-SHA-1 value. Dynamic truncation (DT) is then used to convert the 20-byte text into a 4-byte string. The following is how the 4-byte string is produced: The offset bits (Offset) are first retrieved from String [19]'s low-order 4 bits. The next step is to create the 4-byte string P, which is formed from String [Offset] to String [Offset+3]. P's final 31 bits (or its shortened 4 bytes) are then returned.

The TOTP value is computed in the following manner: first, S is converted to a number Snum in the range 0 to 2^{31}-1. Next, D is computed as the remainder when Snum is divided by 10^{Digit}. Here, Digit is a variable that specifies the number of digits in the OTP. The proposed OTP authentication scheme involves three phases: OTP generation, OTP encryption using (3,3) VCC, and OTP decryption using PVC. To generate the OTP, a synchronous technique called HMAC OTP (HOTP) generation is used. The HOTP is generated by computing the time difference, generating a HMAC-SHA-1 value, and then using dynamic truncation to generate a 4-byte string. Finally, the TOTP value is computed by converting S to a number Snum and then computing D as the remainder when Snum is divided by 10^{Digit}.

In the proposed framework, a Visual Cryptography Schema technique is opted for securing divide the resulting OTP image into three parts. It includes three steps - firstly, an OTP is generated , then it is encrypted using visual cryptography, and then finally decrypted to retrieve the original text

A. OTP GENERATION TECHNIQUE

The first part of the framework had three main steps -

1. A time-based OTP with a growing counter value is generated [20].
2. An HOTP value was created using HMAC-SHA-1 technique. In this technique, a symmetric key was used for the encryption.
3. The 160 bits of the output was reduced to 32 bits.

Algorithm:

Step I: Calculate an HMAC-SHA-1 number by utilising T, the variance between the starting counter time (t1) and the current system time (t2), and k, the encryption secret key.

Step II: The output generated in step i is 160 bits long. Since it is quite inconvenient for the user to enter such a long OTP, thus we reduce it to 32 bits (4 bytes). To do this, Dynamic truncation is done.

Step III: Following are the steps used in DT -

1. HS is the output in step i (132 bits long), which when passed to the function DT, gives the output S. This output is just 4 bytes long.

$$S = DT\ (HS) \qquad (1)$$

2. HS is string of 20 bytes, that is, Strings [0] through [19]. Allow bits to be offset Let Offset be the low-order four bits of String [19], so that:

$$Offset = StToNum\ (OffsetBits) \qquad (2)$$
$$where\ 0 \le Offset \le 15$$

3. Assume P = String [OffSet]...Return the final 31 bits of P (the truncated 4 bytes) after String[OffSet+3].

Step IV: Finally, a time based OTP is calculated using these steps -

1. Convert S to a number in 0...2^ {31} -1, let the number be Tno.

$$D = Tonomod\ 10\text{^}Digit \qquad (3)$$
$$where\ D\ is\ a\ number\ is\ the\ range\ 0 \ldots .10^{\{Digit\}} - 1$$

B. OTP ENCODING AND DECODING USING VISUAL CRYPTOGRAPHY

Using traditional VCS technique, we used two codebooks which were the matrices C0 and C1.

$$C0 = \begin{matrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} \quad C1 = \begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix} \qquad (4)$$

Here C0 denoted the shares of white pixels of the image and c1 denoted the shares of black pixels of the image. The below flowchart(Figure 2) shows the encryption of the OTP

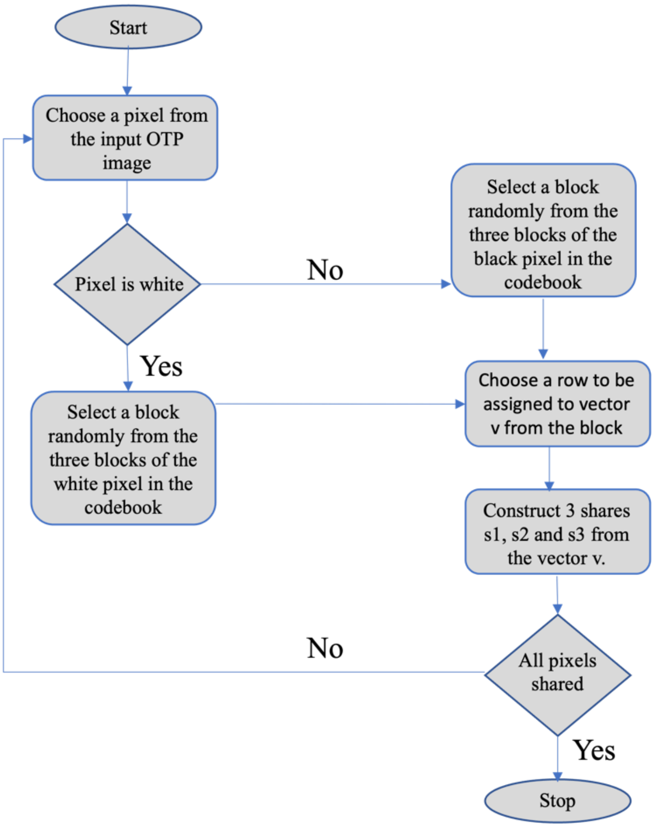

Start
Choose a pixel from the input OTP image
Pixel is white
No
Select a block randomly from the three blocks of the black pixel in the codebook
Yes
Select a block randomly from the three blocks of the white pixel in the codebook
Choose a row to be assigned to vector v from the block
Construct 3 shares s1, s2 and s3 from the vector v.
No
All pixels shared
Yes
Stop

Figure 2 – OTP Encryption Flowchart

Utilising the XOR operation and PVC method, all three shares are joined to create the hidden image R.

$Result = share1 \oplus share2 \oplus share3$ *or* $share1 \oplus share3 \oplus share2$ *or* $share2 \oplus share1 \oplus share3$ *or* $share2 \oplus share3 \oplus share1$ *or* $share3 \oplus share1 \oplus share2$ *or* $share3 \oplus share2 \oplus share1.$ *(5)*

VI. RESULT AND DISCUSSION

In Figure 3, an OTP image was generated using the HOTP creation method. However, due to its encryption using the (3,3) VCS, the resulting OTP is not visible to users. Figure 4 illustrates how the OTP image was partitioned into multiple shares. Users can access only one of these shares, while the remaining shares are stored on the server in different locations. The process of generating OTPs begins with the creation of an OTP image using the HOTP creation approach, as described in the previous section. This image is then encrypted using the (3,3) VCS technique to make it invisible to users. The (3,3) VCS encryption process splits the OTP image into multiple shares, and each share is encrypted using a unique combination of pixels in the image. To access the OTP, the user must have one share of the image. This share is retrieved from the server, and the user's device applies an algorithm to combine the retrieved share with the user's share. This algorithm uses the combination of pixels that was used to encrypt the share to reconstruct the original OTP image.

The use of multiple shares and the distribution of these shares across different locations on the server enhances the security of the OTP. If an attacker gains access to the server and retrieves one share, they cannot reconstruct the OTP without access to the remaining shares. This method adds a layer of protection while making it harder for hackers to obtain the OTP without authorization.

In conclusion, the use of the (3,3) VCS encryption technique, along with the distribution of OTP image shares across multiple locations on the server, increases the OTP authentication system's security. The resulting OTP is invisible to users, and attackers cannot gain access to the OTP without access to all shares.

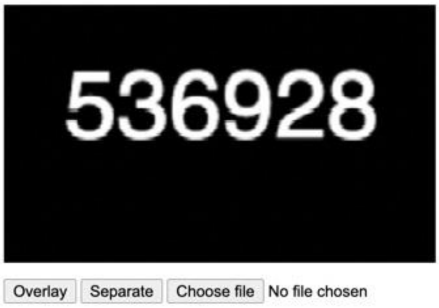
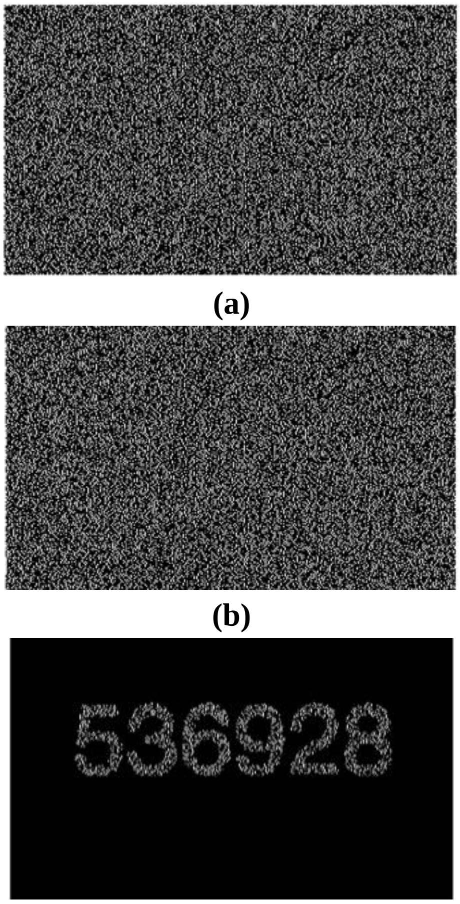


Figure 3 – OTP Image Generated



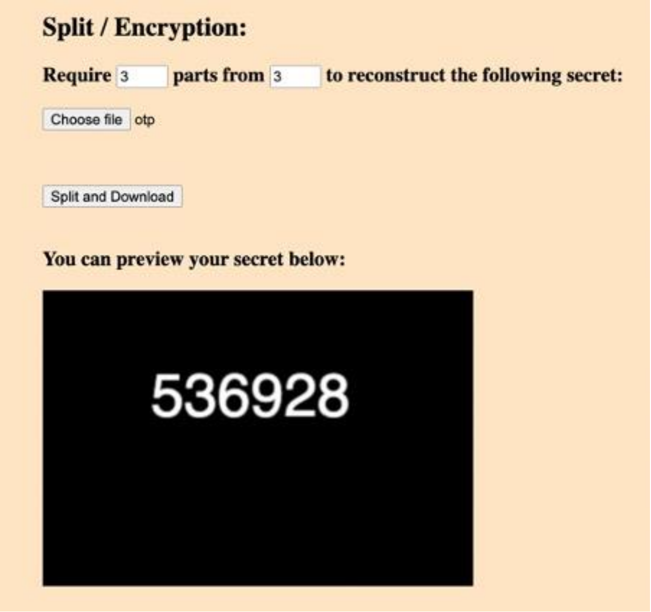
(a)

(b)

(c)

Figure 4 – Encrypted Shares using (3,3) VCS Technique

Once the user uploads their OTP share, the server will validate it and if it matches the initial share, it will fetch the other shares and gradually layer them using the PVC technique until the final OTP image is displayed to the user. On the server side, the OTP is selected and encrypted as shown in Fig. 5, and the user is expected to download an OTP share, which is a set of encrypted shares.



Split / Encryption:

Require 3 parts from 3 to reconstruct the following secret:

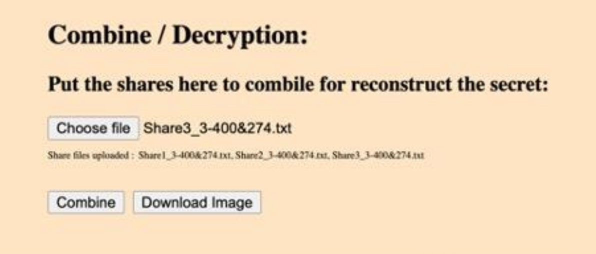
Choose file otp

You can preview your secret below:

536928

Figure 5 – OTP Image Generated

As indicated in Figure 6, the decryption procedure will occur on the client side, and it is anticipated that the downloaded share will be published via the web interface.



Combine / Decryption:

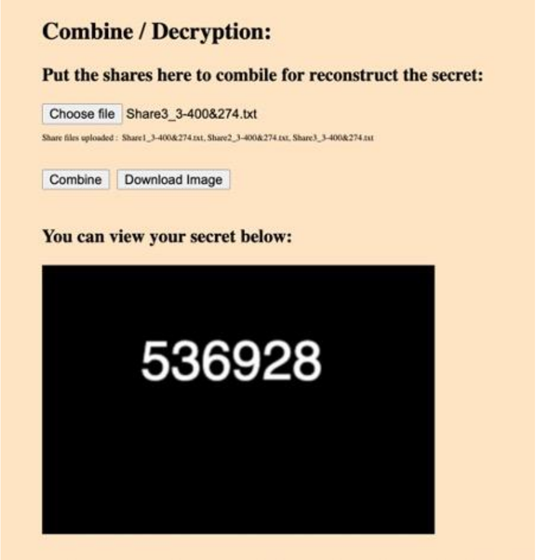
Put the shares here to combile for reconstruct the secret:

Choose file Share3_3-400&274.txt

Share files uploaded : Share1_3-400&274.txt, Share2_3-400&274.txt, Share3_3-400&274.txt

Figure 6 – OTP Shares Upload Interface

Resultant OTP is displayed to user once all the shares have been successfully combined, as illustrated in Figure 7.



Combine / Decryption:

Put the shares here to combile for reconstruct the secret:

Choose file Share3_3-400&274.txt

Share files uploaded : Share1_3-400&274.txt, Share2_3-400&274.txt, Share3_3-400&274.txt

You can view your secret below:

536928

Figure 7 – Decrypted shares and OTP is displayed.

VII. PRESENT SCOPE

In defence, during a missile launch, whenever an important action needs to be taken the entire control of the execution can't be handed over to a single individual. Therefore, using our application we can give each person his/her respective share. Any action can be taken only when all the shareholders make an approval, and all the shares are combined to initiate a process. Here, no individual has all the power with himself/herself.

This application can also be used in the banking sector. Suppose two people have a joint account. Now, the person who has his/her phone number linked with the account has all the power to make any transaction even if the other person disagrees. Our OTP framework allows equal distribution of power to both the parties, which means, any transaction would be made only if both the persons agree by sharing their shares of secret code.

Similarly, the framework has its real time application for many top-level confidential data protections.

VIII. CONCLUSION

The protection of OTPs against various threats is a crucial aspect that has been discussed in this paper. The study explored various existing methods and proposed the use of the (3,3) VCS technique to further enhance the security of OTPs. The OTP generation technique employed was the HOTP, which utilizes a static symmetric secret key and a growing counter value. The generated OTP was divided into three shares, with the user holding one of the shares, and the other shares securely kept on the server. To address the issue of pixel enlargement, a gradual layering approach was used to restore the original OTP image.
Overall, the proposed approach provides an effective solution to secure OTP images. However, there is still a need for further research to evaluate the performance of the technique in real-world scenarios. Future research can also focus on improving the speed and efficiency of the OTP generation and encryption process. Additionally, incorporating machine learning techniques to identify potential attacks and vulnerabilities can be explored to further enhance the security of OTPs. In conclusion, this study has demonstrated the potential of the (3,3) VCS technique to secure OTP images, and there is a need for continued research to further improve OTP security.

VIII. REFERENCES

1. S. Prabhu and V. Shah, "Authentication using session based passwords," Procedia Computer Science, vol. 45, pp. 460-464, 2015.
2. A. O. C. Abikoye, H. A. Dokoro, and N. O. Akande, "Modified Advanced Encryption Standard Algorithm for Information Security," Journal of Applied Science and Engineering, vol. 22, no. 2, 2019.
3. H. Liu and Y. Zhang, "An Improved One-time Password Authentication Scheme," in Proceedings of 15th IEEE International Conference on Communication Technology, 2013, pp. 1-5.
4. A. Aboshosha, K. A. El-Dahshan, E. K. Elsayed, and A. A. Elngar, "Multi-channel user authentication protocol based on encrypted hidden OTP," International Journal of Computer Science and Information Security, vol. 13, no. 6, pp. 14-19, 2015.
5. C. Y. Wai, W. Susilo, M. H. Au, and A. M. Barmawi, "A visual one- time password authentication scheme using mobile devices," in Proceedings of the 16th International Conference on Information

and Communications Security (ICICS 2014), L. C. K. Hui, S. H. Qing, Shi E, and Yiu S. M., Eds. Switzerland: Springer International Publishing, 2015, pp. 243-257.

6. M. Thomas and V. Panchami, "An encryption protocol for end-to-end secure transmission of SMS," in International Conference on Circuits, Power and Computing Technologies (ICCPCT-2015), 2015, pp. 1-6.
7. K. K. Kumbhare and K. V. Warkar, "A review on noisy password, voiceprint and One-Time Password," Procedia Computer Science, vol. 78, pp. 382-386, 2016.
8. R. Isawa and M. Morii, "One-Time Password Authentication Scheme to Solve Stolen Verifier Problem," Information Processing Society of Japan and The Institute of Electronics, Information and Communication Engineers, pp. 225-228, 2011.
9. A. R. L. Reyes, E. D. Festijo, and R. P. Medina, "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, vol. 10, no. 1, pp. 242-247, 2018.
10. C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert, "SMS-based one-time passwords: Attacks and defense," in DIMVA, K. Rieck, P. Stewin, and J.-P. Seifert, Eds., vol. 7967. Springer Publishers, 2013, pp. 150-159.
11. P. Singh and B. Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud," Information Sciences, vol. 422, pp. 77-97, 2018.
12. P.-L. Chiu and K.-H. Lee, "User-friendly threshold visual cryptography with complementary cover images," Signal Processing, vol. 108, pp. 476-488, 2015.
13. M. E. Hodeish, L. Bukauskas, and V. T. Humbe, "An optimal (k, n) visual secret sharing scheme for information security," Procedia Computer Science, vol. 93, pp. 760-767, 2016.
14. K. Dhiman and S. Kasana, "Extended visual cryptography techniques for true color images," Computers and Electrical Engineering, pp. 1-12, 2017.
15. S. Hamdare, V. Nagpurkar, and J. Mittal, "Securing SMS Based One Time Password Technique from Man in the Middle Attack," International Journal of Engineering Trends and Technology, vol. 11, no. 3, pp. 154-158, 2014.
16. A. M. Qadir and N. Varol, "A review on cryptography," 2019.
17. D. Mahto and D. K. Yadav, "Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Finger-Print Biometric," in 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), pp. 301-306, 2015.
18. D. Mahto and D. K. Yadav, "Security Improvement of One-Time Password Using Crypto-Biometric Model," in Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics, Smart Innovation, Systems and Technologies, Springer India, pp. 347-353, 2016.
19. S. Prayla Shyry, M. Mahithaasree, and M. Saranya, "Implementation of One Time Password by 3 3 Vedic Multiplier," in International Conference on Computer, Communication, and Signal Processing, 2018.
20. D. Zhao and W. Luoa, "One-time password authentication scheme based on the negative database," Engineering Applications of Artificial Intelligence, vol. 62, pp. 396-404, 2017.
21. T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," IEEE, 2020.

22. K. Halunen and O.-M. Latvala, "Review of the use of human senses and capabilities in cryptography," 2021.Transactions on Knowledge and Data Engineering, 31(12), 2355-2368. DOI: 10.1109/TKDE.2019.2919844
23. Alkhalifa, E., Aloulou, H., & Mohamed, A. (2019). Towards Building an Intelligent Job Recommendation System for the Arab World. 2019 IEEE 3rd Middle East and Africa Conference on Biomedical Engineering (MECBME). doi: 10.1109/MECBME.2019.8760938