



VIT[®]
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Submitted towards J component of the course
Network and Information Security
ITE4001

Under the guidance of
Dr. JEYANTHI N
Associate Professor Sr.

Submitted by
Dhaval Mavani (19BIT0316) G1/TG1
Aadi Manchekar (19BIT0323) G1/TG1
Muskan Kasera (19BIT0324) G2/TG2

Review 3
Enhanced Authentication for Dynamic Password
Generation using QR code

Abstract

In today's day and age, all of us have had many technological gifts in our hands which our predecessors did not. The rise in technological advancements while doing a lot of good have many contingencies which can cause a lot of harm. In this project we come up with a way to provide an authentication method which uses Dynamic Password Generation using the QR code technology which is readily accessible to anyone who has a phone these days. We developed EADPQR(Enhanced Authentication for Dynamic Password generation using QR code).

EADPQR is an Enhanced method for generation and transmission of OTP(One time password) over any protocol.

Keywords- Dynamic Password, QR code, Authentication, EADPQR, Security

Problem Statement

As the times are changing the ways of authentication need to change with them as well. Hackers and exploiters have become much smarter over the past decade and so have their tools. They have more resources than ever before and this is why we need to step up our security measures to counter these.

Our project idea focuses on one such way in which passwords for certain login events are generated on the spot dynamically and the same is then converted into a QR code which then again undergoes through superimposing of it by another QR code. This is then sent through the network as a distorted QR code which when it receives the recipient from the sender can be retrieved using a mechanism to undo the distortion.

Using an idea like this will help us protect our accounts, data etc while also not needing to remember passwords or saving them anywhere they can all be accessed. Our project tackles two big issues in the cybersecurity world. How to circumnavigate man in the middle attacks as well as making it difficult for anyone to access your account as the password is not saved in a conventional way.

Background

The project is based mostly on the two technologies of Dynamic password generation and QR code generation while also relying on superimposition of the same.

“A QR code (an initialism for Quick Response code) is a type of matrix barcode (or two- dimensional barcode) invented in 1994 by the Japanese automotive company Denso Wave. A barcode is a machine-readable optical label that contains information about the item to which it is attached.” [1]

The QR code contains a white background image on which black squares are arranged in a way which can be read by the camera of any device. The orientation of the same is also not important as they can be read vertically as well as horizontally.

An example of the same is given below:



Figure-1: QR code

“The way that dynamic passwords work is based on the authentication method, it will send you a code that only works once, expires within a short time period, and makes it more difficult for hackers to access your account.

Common examples of authenticators that use OTPs are Google Authenticator and Microsoft Authenticator which give you a 6 digit code that you have one minute to use to access a login like Salesforce.” [2]

Literature Survey

Author/ Name	Title	Summary	Reference
1) M. H. S. AbouSteit, A. F. Tammam and A. Wahdan	A Novel Approach For Generating One-Time Password With Secure Distribution	In this paper the authors have come up with a variation of OTP(one time password) which does not send the OTP as it is but instead uses encryption methods to encrypt the OTP before sending it making it more secure.	M. H. S. AbouSteit, A. F. Tammam and A. Wahdan, "A Novel Approach For Generating One- Time Password With Secure Distribution," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 461-466, doi: 10.1109/WorldS450073.2020.9210322. [3]
2) D. Pansa and T. Chomsiri	Dynamic Password Authentication: Designing step and security analysis	In this paper the authors focused on the viability of the various dynamic password authentication methods and it they were as reliable and effective as the traditional methods. The paper finally concludes that dynamic password authentication methods are viable in websites etc.	D. Pansa and T. Chomsiri, "Dynamic Password Authentication: Designing step and security analysis," 2012 7th International Conference on Computing and Convergence Technology (ICCCT), 2012, pp. 518-523. [4]
3) M. Shakir and A. A. Khan	Scalable shoulder-surfing resistant textual-formula base password authentication system	In this paper the authors have made a formula that changes a normal password into a more secure password that is difficult to remember or be accessed by shoulder surfing which is a very common way passwords are stolen.	M. Shakir and A. A. Khan, "S3TFPAS: Scalable shoulder-surfing resistant textual-formula base password M. Shakir and A. A. Khan, "S3TFPAS: Scalable shoulder-surfing resistant textual-formula base password

4) G. S. K. Fung, R. W. H. Lau and J. N. K. Liu	A signature based password authentication method	In this paper the authors have come up with an additional step while entering password in which the computer will ask the user to enter their signature as well digitally and the same is then used to identify if the person entering the password is the real user or just someone trying to appear as him/her.	G. S. K. Fung, R. W. H. Lau and J. N. K. Liu, "A signature based password authentication method," 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, 1997, pp. 631-636 vol.1, doi: 10.1109/ICSMC.1997.625824. [6]
5) D. Pansa and T. Chomsiri	Integrating the Dynamic Password Authentication with Possession Factor and CAPTCHA	In this paper the authors have made it so that the CAPTCHA question instead of being present in the same page as the password input is instead mailed to the user through their email ID and answered through the mail directly making it more resilient to pass as someone else.	D. Pansa and T. Chomsiri, "Integrating the Dynamic Password Authentication with Possession Factor and CAPTCHA," 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS), 2018, pp. 530-535, doi: 10.1109/SCIS-ISIS.2018.00093. [7]
6) Bertrand Cambou, David Hély, Sareh Assiri	Cryptography with Analog Scheme Using Memristors	In This Paper, The suggested encryption techniques produce cyphers that can only be decrypted by the same memristors or their pictures stored in different devices by directly using memristor arrays or their photographs. It employs a Digital-to-Analog conversion that takes use of the characteristics of low-current memristor cells. In the future, the study will focus on developing larger memristor arrays that are optimised for low power in the 64-KB region, as well as designing encrypting devices that can handle longer messages in the Mbyte level.	Cambou, Bertrand, David Hély, and Sareh Assiri. "Cryptography with analog scheme using memristors." ACM Journal on Emerging Technologies in Computing Systems (JETC) 16, no. 4 (2020): 1-30. [8]

7) MARCO VASSEN, CRAIG DISSELKOE N, KLAUS VON GLEISSENT HALL, SUNJAY CAULIGI, RAMI GÖKHAN KICI, RANJIT JHALA DEAN TULLSEN, DEIAN STEFAN	Automatically eliminating speculative leaks from cryptographic code with blade	Blade, a completely automated technique to provably and efficiently reduce speculation- based leakage in unannotated cryptographic code, is presented in this work. Blade identifies data flows from transient sources to steady sinks statically and generates a small number of fence- based or SLH- based protect calls to prevent leaks. Our tests demonstrate that Blade adds an order of magnitude less safeguards than today's compilers, and that existing crypto primitives mended with Blade have only minor overheads when utilising fences and SLH for protect.	Vassena, Marco, Craig Disselkoe, Klaus von Gleissenthall, Sunjay Cauligi, Rami Gökhan Kıcı, Ranjit Jhala, Dean Tullsen, and Deian Stefan. "Automatically eliminating speculative leaks from cryptographic code with blade." Proceedings of the ACM on Programming Languages 5, no. POPL (2021): 1-30. [9]
8) Zeng, Jianhua, Yanlin Zhan, and Jianrong Yang.	Encryption and Decryption of Optical Images with Different Algorithms	While digital images are the most prevalent type of information on the internet, their security is a major problem, and image encryption technology is one of the most important tools for ensuring image security. To investigate the encryption and decryption of optical images using MATLAB, the following methods were used: randomly disrupting the row or column of each layer; randomly disrupting the pixel points; scaling the RGB values of pixel points; transposing, horizontal flipping, and vertical flipping of RGB matrixes; and the one- dimensional and two- dimensional data reset of RGB matrixes. Different encryption algorithms have different image encryption effects and operating speeds. The research is to better assess this technology for beginners who are interested in image encryption and decryption technologies and to lay the foundation for these individuals to develop more advanced encryption and decryption technologies in the future.	Zeng, Jianhua, Yanlin Zhan, and Jianrong Yang. "Encryption and Decryption of Optical Images with Different Algorithms." In Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture, pp. 256-265. 2020. [10]

9) Malik, Muhammad Wito, Diyanatul Husna, I. Ketut Eddy Purnama, Ingrid Nurtanio, Afif Nurul Hidayati, and Anak Agung Putri Ratna.	Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method	The development of medical picture encryption technologies is discussed in this thesis. The histogram, as well as the correlation coefficient, are used to compare the distribution of values and the number of pixels in the original picture with the image after processing, and to assess the correlation between pixels in the image. Based on the results of the tests, the Medical Image Encryption System Using the AES Encryption Method will generate a randomised new image with an average RMS Error of 4388.39, a horizontal correlation coefficient of 0.03344, a vertical correlation coefficient of 0.00742, and a diagonal correlation coefficient of 0.01110.	Malik, Muhammad Wito, Diyanatul Husna, I. Ketut Eddy Purnama, Ingrid Nurtanio, Afif Nurul Hidayati, and Anak Agung Putri Ratna. "Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method." In 2020 the 6th International Conference on Communication and Information Processing, pp. 153-158. 2020. [11]
10) Gong, Bo-fan.	Hybrid Compression and Lightweight Encryption of Color Image	In This paper author offers a transform-domain technique for encrypting pictures. The RGB colour image is first converted to YUV, after which the Arnold transformation is performed using 8x8 size blocks as the fundamental unit to scramble the pixel position, and each block is then DCT transformed and quantified. Finally, to accomplish data compression, the quantization results are encoded using run-length and differential coding, and the final result is produced by encrypting the coded data using the RC4 stream cypher. The encryption technique includes the following features: a wide key space, the ability to mix the YUV three colour gamuts, and the ability to combine with the image's transform domain. Accordingly, the security is high. In addition, the results of the experiments show that the algorithm runs fast and the pixel value distribution of cipher text image is more uniform, that is, the encryption effect is good.	Gong, Bo-fan. "Hybrid Compression and Lightweight Encryption of Color Image." In Proceedings of the 2020 5th International Conference on Multimedia Systems and Signal Processing, pp. 36-39. 2020. [12]

11) M. Karnan and N. Krishnaraj	Bio password-Keystroke dynamic approach to secure mobile devices	In this paper the authors focus on the variations in keystrokes in different individuals. The methodology that they use makes use of the rhythm which is habitually displayed by a particular person.	M. Karnan and N. Krishnaraj, "Bio password — Keystroke dynamic approach to secure mobile devices," 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010, pp. 1-4, doi: 10.1109/ICCIC.2010.5705901. [13]
12) Yi-Pin Liao, Shuenn- Shyang Wang	A secure dynamic ID-based remote user authentication scheme for multi-server environment	In this paper, the authors focus on the usage of IDs in a remote way as a method of authentication. It is focused more on the multi server environments. The given methodology uses only hashing to do so too.	Yi-Pin Liao, Shuenn-Shyang Wang, A secure dynamic ID based remote user authentication scheme for multi- server environment, Computer Standards & Interfaces, Volume 31, Issue 1, 2009, Pages 24-29, ISSN 0920-5489, https://doi.org/10.1016/j.csi.2007.10.007 . (https://www.sciencedirect.com/science/article/pii/S0920548907001043) [14]
13) Kurogi T., Yamaba H., Aburada K., Katayama T., Park M., Okazaki N.	A Study on a User Identification Method Using Dynamic Time Warping to Realize an Authentication System by s-EMG	In this paper the authors focus on the usage of s-EMG which is a type of electromyogram for the authentication of a user. It uses gestures as a means of authentication using the same technology.	Kurogi T., Yamaba H., Aburada K., Katayama T., Park M., Okazaki N. (2018) A Study on a User Identification Method Using Dynamic Time Warping to Realize an Authentication System by s-EMG. In: Barolli L., Khafa F., Javaid N., Spaho E., Kolici V. (eds) Advances in Internet, Data & Web Technologies. EIDWT 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 17. Springer, Cham. https://doi.org/10.1007/978-3-319-75928-9_82 [15]

14) Alpar O., Krejcar O	Pattern Password Authentication Based on Touching Location	In this paper the authors focus on the usage of patterns which is already in use for a long time but with the added functionality of checking the touching location as well as the angle at which each edge is inputted.	Alpar O., Krejcar O. (2015) Pattern Password Authentication Based on Touching Location. In: Jackowski K., Burduk R., Walkowiak K., Wozniak M., Yin H. (eds) Intelligent Data Engineering and Automated Learning – IDEAL 2015. IDEAL 2015. Lecture Notes in Computer Science, vol 9375. Springer, Cham. https://doi.org/10.1007/978-3-319-24834-9_46 [16]
15) X. Liu, T. Huang, X. Wang and X. Tang	A user authentication scheme based on dynamic password for wireless sensor networks	In this paper the authors focus on the usage of schemes while implementing the dynamic password system especially made for the wireless sensor networks. It uses the one way hash function as well as x-OR operations.	X. Liu, T. Huang, X. Wang and X. Tang, "A user authentication scheme based on dynamic password for wireless sensor networks," 2010 International Conference on Intelligent Computing and Integrated Systems, 2010, pp. 145-148, doi: 10.1109/ICISS.2010.5656792. [17]
16) Velásquez, Ignacio & Caro, Angelica	Authentication Schemes and Methods: a Systematic Literature Review	In this paper the authors have done a systematic literature review on the various authentication schemes and methodology. It has accounted for 515 single factor and 442 multi factor methodologies used for authentication.	Velásquez, Ignacio & Caro, Angelica & Rodríguez, Alfonso. (2017). Authentication Schemes and Methods: a Systematic Literature Review. Information and Software Technology. 94. 10.1016/j.infsof.2017.09.012. [18]
17) Yohan Muliono, Hanry Ham, Dion Darmawan	Keystroke Dynamic Classification using Machine Learning for Password Authorization	In this paper the authors have used Machine Learning while focusing on the keystroke for the authorization of a person. It relies on the fact that each individual has a different keystroke pattern on the basis of which they can be differentiated.	Yohan Muliono, Hanry Ham, Dion Darmawan, 2018, Keystroke Dynamic Classification using Machine Learning for Password Authorization, Procedia Computer Science 135 (2018) 564–569 [19]

18) Geng B., Ge L., Wang Q., Wang L	Improved Digital Password Authentication Method for Android System	In this paper the authors have focused on the improvement of the existing password authentication method which is used in the Android system. It does so by introducing random numbers as well as increasing the number of constant numbers.	Geng B., Ge L., Wang Q., Wang L. (2018) Improved Digital Password Authentication Method for Android System. In: Huang DS., Jo KH., Zhang XL. (eds) Intelligent Computing Theories and Application. ICIC 2018. Lecture Notes in Computer Science, vol 10955. Springer, Cham. https://doi.org/10.1007/978-3-319-95933-7_86 [20]
19) Orcan Alpar	Intelligent biometric pattern password authentication systems for touchscreens, Expert Systems with Applications	In this paper the author makes case for a biometric pattern password authentication system designed specifically for devices with touch screens. The author uses classifier algorithms such as ANN, ANFIS and RGB Histogram.	Orcan Alpar, Intelligent biometric pattern password authentication systems for touchscreens, Expert Systems with Applications, Volume 42, Issues 17–18, 2015, Pages 6286-6294, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2015.04.052 . (https://www.sciencedirect.com/science/article/pii/S0957417415002948) [21]
20) Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee, Thian Song Ong	Keystroke dynamics in password authentication enhancement	In this paper the authors use the keystroke dynamics as an added authentication method with the preexisting password input. They use multiple dynamic framework under a fusion framework to achieve the same.	Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee, Thian Song Ong, Keystroke dynamics in password authentication enhancement, Expert Systems with Applications, Volume 37, Issue 12, 2010, Pages 8618-8627, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2010.06.097 . (https://www.sciencedirect.com/science/article/pii/S0957417410006019) [22]

21) C. Wang and C. Feng	Security Analysis and Improvement for Kerberos Based on Dynamic Password and Diffie-Hellman Algorithm	In this paper the authors work on a Kerberos based on Dynamic password as well as the Diffie-hellman algorithm. It uses the idea of the interaction between the client and Kerberos key distribution center and making the password exchanges using the algorithm.	C. Wang and C. Feng, "Security Analysis and Improvement for Kerberos Based on Dynamic Password and Diffie-Hellman Algorithm," 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013, pp. 256-260, doi: 10.1109/EIDWT.2013.49. [23]
22) Aaron L.-F. Han, Derek F. Wong, Lidia S. Chao	Advances of Password Cracking and Countermeasures in Computer Security	In this paper the authors discuss and survey on the advancements in the password cracking as well as the countermeasure security for the same that has been iterated over the years.	Aaron L.-F. Han, Derek F. Wong, Lidia S. Chao, 2020, Advances of Password Cracking and Countermeasures in Computer Security, NLP2CT Lab, University of Macau, Macau SAR ILLC, University of Amsterdam, Science Park 107, 1098 XG Amsterdam [24]
23) J. Weaver, K. Mock and B. Hoanca	Gaze-based password authentication through automatic clustering of gaze points	In this paper the authors come up with the methodology of using gaze-based password authentication with the use of automatic clustering to help. The methodology is also fast with the average time taken for authentication coming at 3 seconds for a 4-digit PIN.	J. Weaver, K. Mock and B. Hoanca, "Gaze-based password authentication through automatic clustering of gaze points," 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2011, pp. 2749-2754, doi: 10.1109/ICSMC.2011.6084072. [25]

24) Andriotis P., Tryfonas T., Oikonomou G	Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method	In this paper the authors discuss about the complexity metrics as well as the perception of strength of the user regarding the Pattern-Lock Graphical authentication methodology. It also glances over the biases the same may have to go through.	Andriotis P., Tryfonas T., Oikonomou G. (2014) Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In: Tryfonas T., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Cham. https://doi.org/10.1007/978-3-319-07620-1_11 [26]
25) L. Wu, T. Chen, C. Qiao and Z. Li	Authentication Technology of Mobile Internet of Things Based on the Dynamic Password	In this paper the authors discuss and come up with the methodology of using Dynamic password in technologies that are included in the IoT(internet of things). The paper talks about a RFID mutual method which when used for authentication resolves fake and heavy attacks.	L. Wu, T. Chen, C. Qiao and Z. Li, "Authentication Technology of Mobile Internet of Things Based on the Dynamic Password," 2018 IEEE International Conference of Safety Produce Informatization (IICSPI), 2018, pp. 204-208, doi: 10.1109/IICSPI.2018.8690463.[27]
26) Kapil Juneja	An XML transformed method to improve effectiveness of graphical password authentication	In this paper the author discusses the usage of an XML transformed method which is used to improve the effectiveness of the graphical password authentication. It focusses on the LSB steganography approach.	Kapil Juneja, An XML transformed method to improve effectiveness of graphical password authentication, Journal of King Saud University - Computer and Information Sciences, Volume 32, Issue 1, 2020, Pages 11-23, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2017.07.002 . (https://www.sciencedirect.com/science/article/pii/S131915781730112X) [28]

27) M. Martinez-Diaz, J. Fierrez and J. Galbally	Graphical Password-Based User Authentication With Free-Form Doodles	In this paper the authors discuss of a way of authentication which uses free form doodles as an Graphical based password for the authentication of an individual. The method does has some high error margins as cited by the authors in the abstract.	M. Martinez-Diaz, J. Fierrez and J. Galbally, "Graphical Password-Based User Authentication With Free-Form Doodles," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 4, pp. 607-614, Aug. 2016, doi: 10.1109/THMS.2015.2504101. [29]
28) Fan C., Bai C., Zou J., Zhang X., Rao L	A Dynamic Password Authentication System Based on NoSQL and RDBMS Combination	In this paper the authors come up with a methodology which is based on NoSQL and RDBMS as a combination for the implementation of a Dynamic password authentication method. The OTP method is based on a combination of the method mentioned above.	Fan C., Bai C., Zou J., Zhang X., Rao L. (2015) A Dynamic Password Authentication System Based on NoSQL and RDBMS Combination. In: Zhang R., Zhang Z., Liu K., Zhang J. (eds) LISS 2013. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40660-7_121 [30]
29) Deng K., Zhang Y	Dynamic Password Authentication Protocol Using Interference Factor	In this paper the authors apply a methodology which uses Interference factor in conjunction with the dynamic password authentication. Indirect authentication is used instead of direct authentication.	Deng K., Zhang Y. (2012) Dynamic Password Authentication Protocol Using Interference Factor. In: Qian Z., Cao L., Su W., Wang T., Yang H. (eds) Recent Advances in Computer Science and Information Engineering. Lecture Notes in Electrical Engineering, vol 127. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25769-8_87 [31]

30) Kiss P.J., Klimkó G	Authentication of Electronic Legal Statements by a Trust Service Provider Using Two-Factor Dynamic Handwritten Signature Verification	In this paper the authors use a two factor methodology which uses Handwritten signature as an input for verification as well as authentication of an individual when accessing Electronic legal statements. This is meant for trust service providers.	Kiss P.J., Klimkó G. (2020) Authentication of Electronic Legal Statements by a Trust Service Provider Using Two-Factor Dynamic Handwritten Signature Verification. In: Kő A., Francesconi E., Kotsis G., Tjoa A., Khalil I. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2020. Lecture Notes in Computer Science, vol 12394. Springer, Cham. https://doi.org/10.1007/978-3-030-
31) Kieseberg, Peter, et al.	QR code security	The purpose of this research is to examine QR Codes and how they can be utilized to target both human and automated systems. A user cannot tell the difference between a genuine and a maliciously modified QR code because the encoded information is designed to be machine-readable only. While people are prone to phishing assaults, robot readers are more likely to be targeted by SQL and command injections.	Kieseberg, Peter, et al. "QR code security." Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. 2010.
32) Shimizu, Akihiro.	"A dynamic password authentication method using a one-way function	A new password-based authentication method has been developed. CINON is being proposed for use in computer and telecommunication systems. To conduct the required authentication of communicating users, it uses a one-way function. In the event of a wiretap or the theft of a password file, CINON's security is maintained, and the correspondents' public passwords are not required to be replaced. Only a few computations are required to realise CINON.	Shimizu, Akihiro. "A dynamic password authentication method using a one-way function." Systems and computers in Japan 22.7 (1991): 32-40. https://doi.org/10.1002/scj.4690220704

33) Singh, Anuraj, and Sumit Raj.	Securing password using dynamic password policy generator algorithm.	In this research, an algorithm is designed for dynamically generating password regulations based on the database's character frequency. The algorithm generates efficient regulations that are unique to each user. In its password area, it employs practically every character that isn't normally utilised. The password that the user creates using the dynamic policy is both strong and complex. It is more difficult for an attacker to crack those passwords.	Singh, Anuraj, and Sumit Raj. "Securing password using dynamic password policy generator algorithm." Journal of King Saud University-Computer and Information Sciences (2019). https://doi.org/10.1016/j.jksuci.2019.06.006
34) Kan, Tai-Wei, Chin-Hung Teng, and Wen-Shou Chou.	Applying QR code in augmented reality applications."	In this research, we describe a QR Code-based augmented reality (AR) application. The system can extract information from a QR Code and display it in a 3D format, with the QR Code serving as the traditional AR marker. Traditional AR systems recover the 3D scene structure and identify the object to be presented on the scene using a specially defined pattern .	Kan, Tai-Wei, Chin-Hung Teng, and Wen-Shou Chou. "Applying QR code in augmented reality applications." Proceedings of the 8th International Conference on Virtual Reality Continuum and its Applications in Industry. 2009.
35) H. Sun, Y. Chen and Y. Lin, "oPass	A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks,	Because of their convenience and simplicity, text passwords are the most used form of user authentication on websites. Users' passwords, on the other hand, are vulnerable to being stolen and compromised due to a variety of risks and vulnerabilities. In this work, we propose oPass, a user authentication system that uses a user's smartphone and short message service to prevent password theft and reuse threats. oPass merely asks that each participating website have a unique phone number and that the registration and recovery phases involve a telecommunication service provider	H. Sun, Y. Chen and Y. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651-663, April 2012, doi: 10.1109/TIFS.2011.2169958.
36) Phaisarn Sutheebanjard, Wichian Premchaiswadi	QR-Code Generator	In this paper, we demonstrate how to produce QR codes using a web browser, allowing users to make their own QR codes for websites, emails, business cards, print ads, and other applications. The proposed solution was built entirely with open source software, including Libqrencode, Drupal, and Ubuntu.	Sutheebanjard, P. & Premchaiswadi, Wichian. (2010). QR-code generator. 89-92. 10.1109/ICTKE.2010.5692920.

37) Sumit Tiwari	An Introduction To QR Code Technology	We investigated QR code technology, its merits, application areas, and impact on the marketing and technological worlds in this article. Originally designed and used for inventory tracking, QR codes have since found uses in a variety of different fields such as marketing, advertising, secure payment systems, education, and so on. Due to advantages such as high data storage capacity, fast scanning, error-correction, direct marking, and convenience of use, QR code adoption has accelerated in recent years, and the number of users has increased significantly.	Tiwari, Sumit. (2016). An Introduction to QR Code Technology. 39-44. 10.1109/ICIT.2016.021.
38) C. Ugwu, T. Mesigo	A Novel Mobile Wallet Based on Android OS and Quick Response Code Technology	We created an Android-based mobile payment system that can be used as a replacement for a physical wallet by allowing users to transfer money between peers. As a form of encryption and communication between the sender and the recipient, the system employs Quick Response codes technology. The system was determined to be more secure due to a better authentication process enforced by many entities, eliminates the need for agents in the payment ecosystem, does not involve sharing of personal information because the QR code handles it, and satisfies the universal property.	Ugwu, CHIDIEBERE & Mesigo, T. (2015). A Novel Mobile Wallet Based on Android OS and Quick Response Code Technology. International Journal of Advanced Research in Computer Science and Technology. 3. 85.
39) Abhishek Mehta, Dr. Kamini Solanki	Design and Development of QR Code Recognition from Digital Image	Due to changes in size, style, orientation, and alignment, as well as low image contrast and a complicated background, QR Code Recognition from photographs is a difficult task. Find a technique for QR code recognition that is both robust and generalised. Many algorithms for identifying QR Code Recognize in an image have been proposed. For a given set of photos, each approach produces reliable findings. Image pre-processing, tilt correction, geometric correction, image normalisation, segmentation and localization, feature extraction, and classification were the methods I utilised to extract patterns.	Abhishek Mehta, Dr. Kamini Solanki 2021 Design and Development of QR Code Recognition from Digital Image international Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181

40) Divya Sharma	A Review of QR code Structure for Encryption and Decryption Process	The production of a QR code using document-based software is the subject of this research paper. A typical user can generate their own QR code for their text in a user-friendly environment of Word, and they can do so by following the methods outlined in this study article. Scanning the Fig 11 QR code with several iPhone readers such as scan life, bee tagg, and others, as well as desktop readers such as Quick Mark and Zxing decoder, and then viewing the information on the user's iphone or desktop.	Divya Sharma, Volume 2, Issue 2, February – 2017 A Review of QR code Structure for Encryption and Decryption Process International Journal of Innovative Science and Research Technology ISSN No: - 2456- 2165
41) Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung, Ting-Ching Lin	A One-Time Password Scheme with QR-Code Based on Mobile Phone	This paper's objective is to be the first to offer a QR code-based one-time password authentication protocol, which not only eliminates the need for a password verification table, but is also a cost-effective solution because most internet users already have mobile phones.	https://www.researchgate.net/publication/221521693_A_One-Time_Password_Scheme_with_QR-Code_Based_on_Mobile_Phone
42) Abey Abraham; Alina Poly; T Aishwarya; Anju George	SPAQ: Secure PIN authentication using QR code	Shoulder-surfing and skimming attacks are very common when employing PIN-based ATM authentication. The purpose is to safeguard ATMs against theft by employing security countermeasures. A three-level verification is used in this article to assure the security of ATM transactions. SPAQ overcomes the security problems associated with PIN-based ATM authentication because it is based on one-time PIN and QR code. In the event that the user's mobile device is lost, the user can also disable the SPAQ service for his account. As a result, the SPAQ service is intuitive and user-friendly.	https://ieeexplore.ieee.org/egateway.vit.ac.in/document/8250661?arnumber=8250661

43) Yaoqiu Hong	Design of Intelligent Access Control System Based on DES Encrypted QR Code	<p>To maintain the security of the QR code, the system converts the input character string using BASE64 conversion technology, then encrypts using the DES method, ensuring optimum information security.</p> <p>A symmetric encryption algorithm, the data encryption standard (DES), is used. DES generates a maximum 64-bit group with a 56-bit key and an additional 8-bit parity. The encrypted text block is split into two halves during the encryption process. The sub-key is used to cycle parts, after which an XOR operation is performed on the output with another part, and the two parts are swapped. This technique is done and cycled over and over again. DES will cycle 16 times, but there will be no exchange in the last cycle. It's quite difficult to crack this encryption.</p>	https://ieeexplore.ieee.org/egataway.vit.ac.in/document/9213475/authors#authors
44) Mete Eminagaoglu; Ece Cini; Gizem Sert; Derya Zor	A Two-Factor Authentication System with QR Codes for Web and Mobile Applications	In this study, it was demonstrated that a one-time QR code verification mechanism may be utilised instead of SMS-based OTPs in all types of web and mobile applications that require two-factor authentication as a practical, effective, and reliable alternative. The model presented and developed in this work also provides substantially larger random data ranges, which may mitigate the relevant cryptographic attack risks that are commonly encountered in ordinary n-digit OTPs.	https://ieeexplore.ieee.org/egataway.vit.ac.in/document/6982784
45) Jisha Thomas; R.H Goudar	Multilevel Authentication using QR code based watermarking with mobile OTP and Hadamard transformation	The internet is the most popular channel for mobile banking services, and the number of people using it will continue to rise. As a result, security must be prioritised, with strong authentication and protection methods in place. Customers should be able to choose their degree of verification more easily. Taking all of this into account, we present a way for strong authentication, as well as a watermarking technique that uses a QR code as the cover picture and an OTP for the watermark's stego key. Hadamard matrix transformations can be used to generate a watermark sequence. Utilizing an Android application, authenticity can be verified in a short period of time using a mobile phone.	https://ieeexplore.ieee.org/egataway.vit.ac.in/document/8554891

Characteristics of QR Code

1. High Capacity encoding data

While conventional bar codes are capable of storing a maximum of approximately 20 digits, QR Code is capable of handling several dozen to several hundred times more information.



2. Small print out size

Since QR Code carries information both horizontally and vertically, QR Code is capable of encoding the same amount of data in approximately one-tenth the space of a traditional barcode.



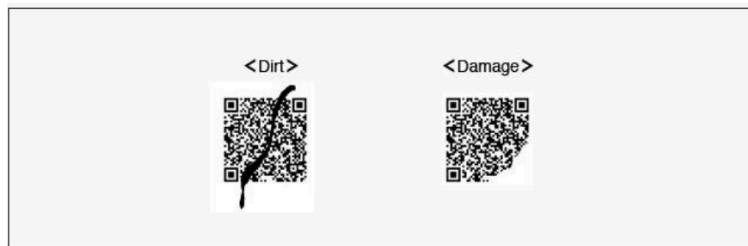
3. Readable from any direction of 360

QR Code is capable of 360 degree (omni-directional), high speed reading. QR Code accomplishes this task through position detection patterns located at the three corners of the symbol. These position detection patterns guarantee stable high-speed reading, circumventing the negative effects of background interference.



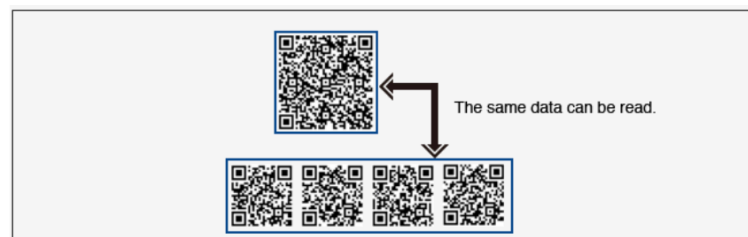
4. Dirt and damage resistant

QR Code has error correction capability. Data can be restored even if the symbol is partially dirty or damaged.



5. Structure appending features

QR Code can be divided into multiple data areas. Conversely, information stored in multiple QR Code symbols can be reconstructed as a single data symbol. One data symbol can be divided into up to 16 symbols, allowing printing in a narrow area.



why not Biometrics/Cliometrics?

Deals with finger prints, Retina scan or Voice/facial recognition this provide good security still they are not used because they are expensive and its authentication process is very slow.

Algorithm

EADP(Enhanced Authentication for Dynamic Password)

The Mathematical Background used in the EADP is Matrices. During the generation of EADP the ASCII characters are stored in a dynamically generated Random matrix which makes the system of security more enhanced as for each iteration the matrix is reshuffled and thus the encryption can't be decrypted easily. Thus it increases the security of the password generated by the program that is by picking up the different elements from the matrix and the matrix at each iteration will get updated by the use of the RANDOM function making the password more secure.

Pseudo Code

Code for the Random Matrix Generation and DYNAMIC OTP

1. Creating List
2. Inserting alphabets, number using (append) and special characters of their
3. Respective ASCII notation in a list by loop.

4. Using Random function inserting elements in a Matrix(8*8), elements will be inserted into the freshly assigned or reshuffled position in the matrix by using the RANDOM function.
5. Getting input of number of digits in OTP.
6. Using random function selecting integral coordinates of form (i ,j) where
7. $0 \leq i \leq 7, 0 \leq j \leq 7$ for each digit in OTP.
8. Fetch the corresponding element from Randomized matrix.
9. Print the corresponding OTP.

FLOWCHART OF EADPQR SCHEME:-

1. EADPQR generates a "N" Digit OTP (Input from Client).
2. This generated OTP is generated by a Randomized matrix method.
3. Another SKIN_OTP ie. a temporary OTP is generated by the same method.
4. This OTP is Superimposed over the Primary QR to Distort the QR.

5. The Distorted QR is Transmitted over the Connection which surpasses all the Decryption patterns using OpenCV libraries.
6. The Transmitted OTP can be Retrieved by end user with Decryption Algorithm

Flow Diagram

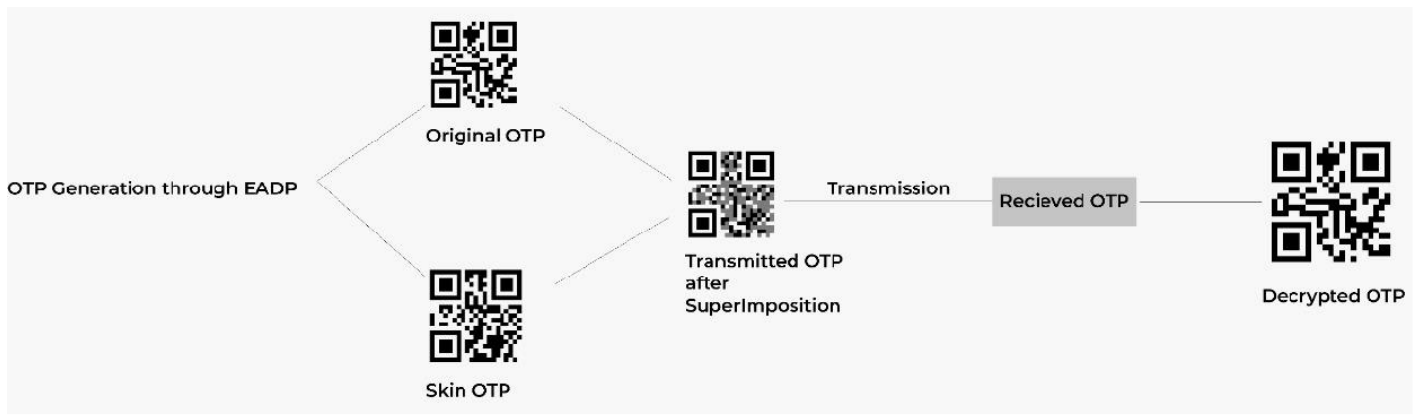
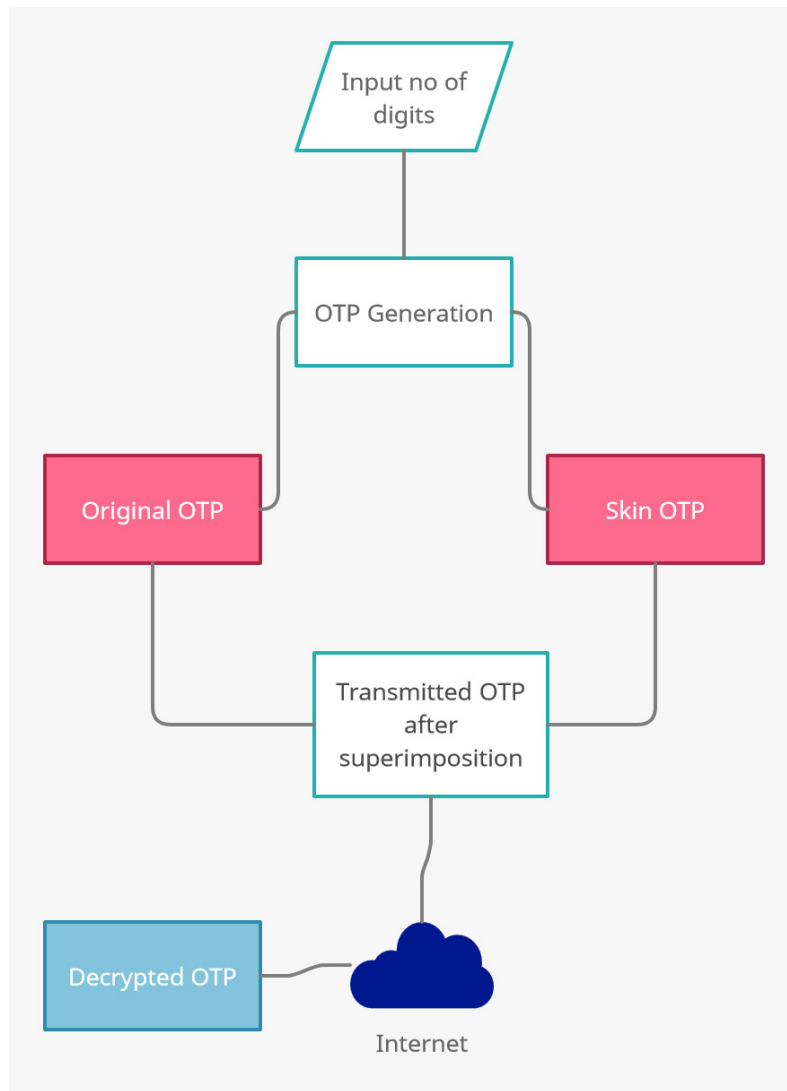
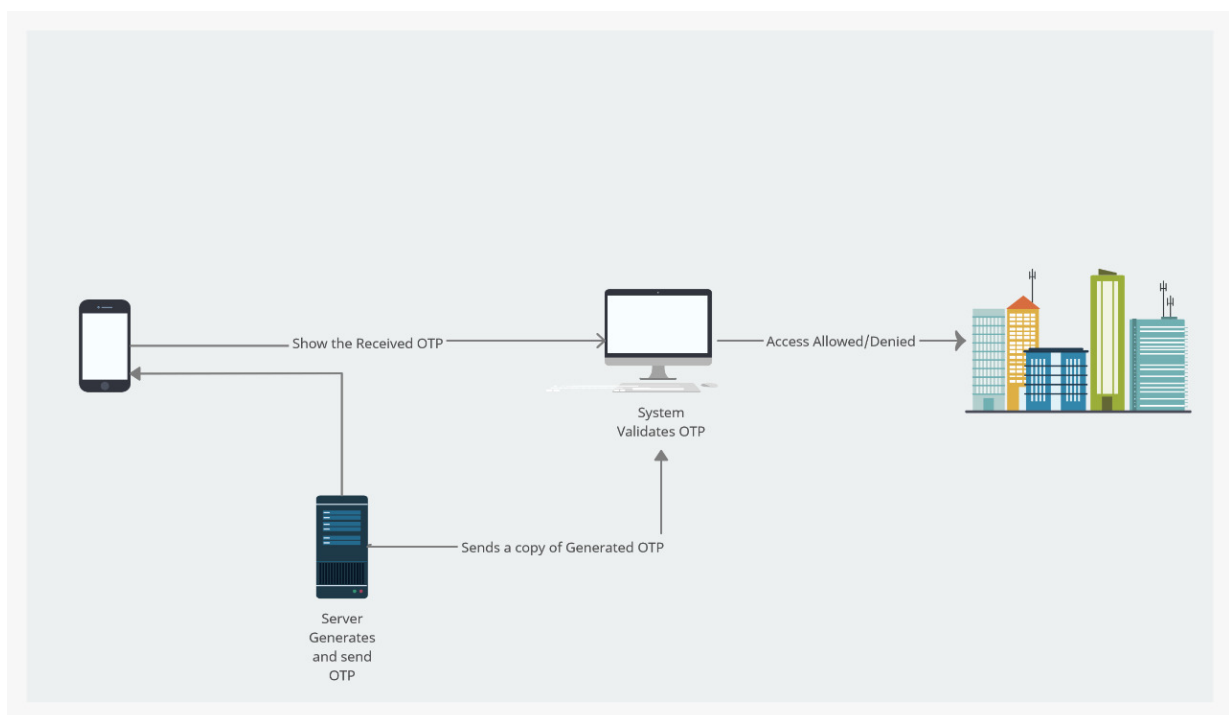


Figure-1: Flow Diagram of the method



System Architecture Diagram



Module Description

The proposed algorithm uses various modules like OpenCV and Numpy. These modules are used to build various parts of code. The OTP is generated through EADP algorithm which was discussed earlier in this paper. From a given n Digit OTP the algorithm then proposes to generate a QR from the given OTP.

OpenCV

OpenCV (Open Source Computer Vision Library) is a free software library for computer vision and machine learning. OpenCV was created to offer a standard infrastructure for computer vision applications and to let commercial goods incorporate machine perception more quickly.

Numpy

NumPy is a Python library used for working with arrays. It also has functions for working in domain of linear algebra, Fourier transform, and matrices. NumPy was created in 2005 by Travis Oliphant. It is an open-source project and you can use it freely. NumPy stands for Numerical Python. The use of above module is to create a matrix and perform various transformations on same.

EADP Scheme Security Analysis

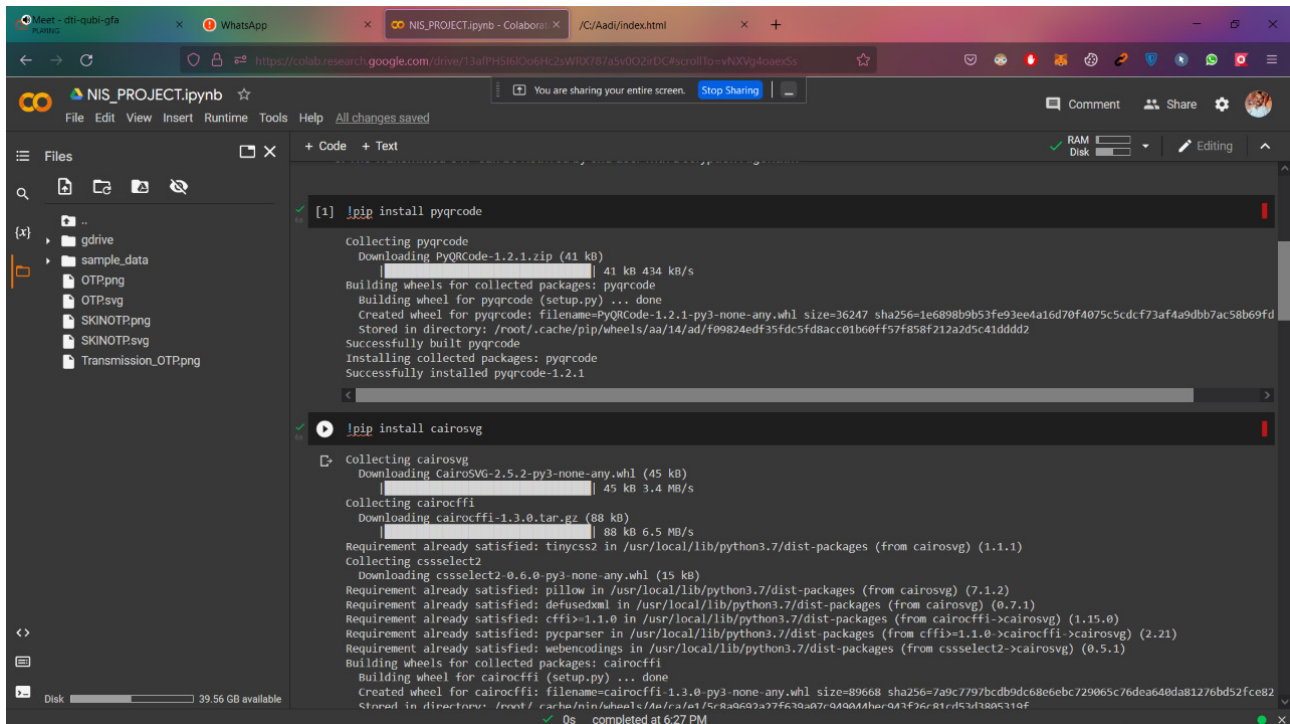
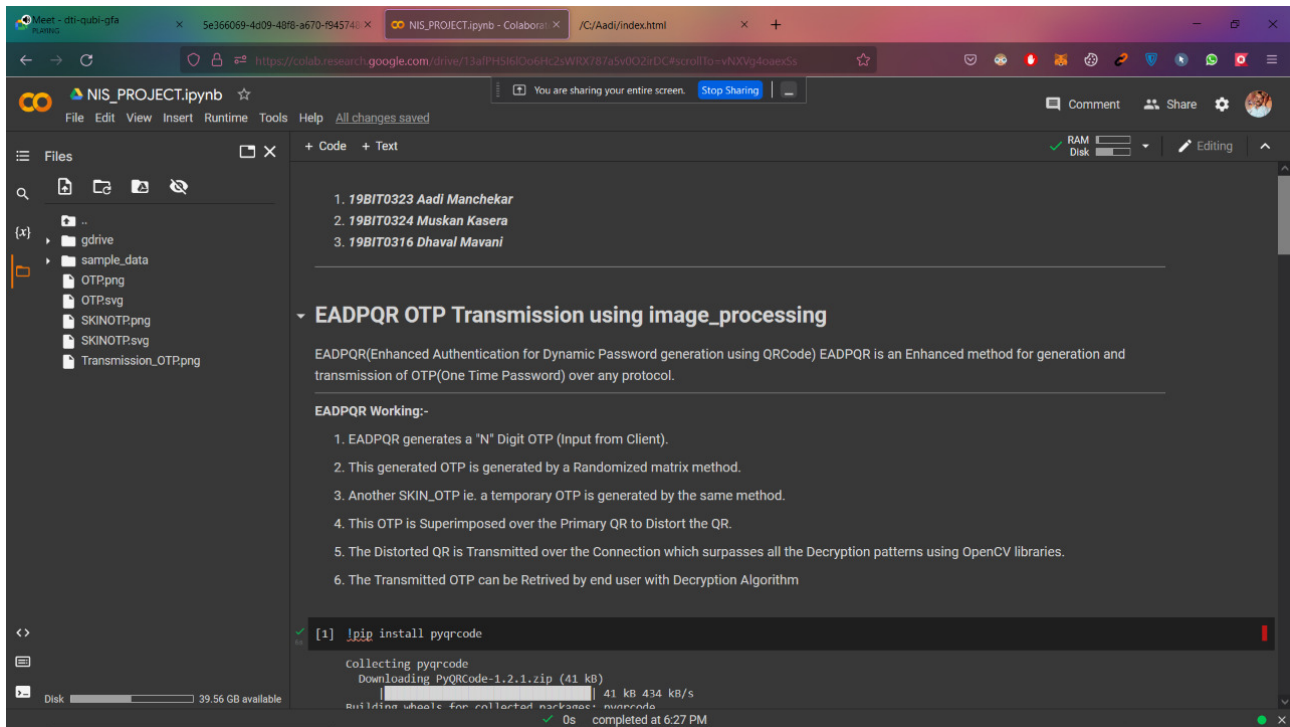
Brute force attack: This strategy entirely eliminates brute force attacks since the password is updated with each login.

Dictionary Attacks: These are password attacks that target character strings. Hackers employ dictionary terms in this attack and authenticate by attempting one word after another in order. Because dynamic passwords are used for each login, dictionary attacks fail against our suggested approach.

Shoulder Surfing: In the proposed approach, randomized alphabet strips mask the password, and Matrix elements are also created randomly, making it totally resistant to Shoulder Surfing or hidden cameras. Even if the password is known, it has already been changed in a fresh session, and it is impossible to establish a new dynamic password without knowing the rating.

Guessing: It is impossible to guess the dynamic password since the displayed strip is randomized with a random number matrix placement in the log in interface.

Snapshots of Implementation and Code



```
import cairosvg
import cv2
import numpy as np
import pyqrcode
from pyqrcode import QRCode
from PIL import Image
import numpy as np

#-----Code for Primary OTP Starts here-----#

flag=0
while(flag==0):
    import random
    q=[]
    a=[x for x in range(65,91)]
    for f in range(48,58):
        a.append(f)
    for e in range(97,123):
        a.append(e)
    a.append(35)
    a.append(42)
    matrix=[]
    for i in range(0,8):
        inArray=[]
        for j in range(0,8):
            c=random.randint(0,len(a)-1)
            a.remove(c)
            inArray.append(chr(c))
            matrix.append(inArray)
        print("Enter The Number of OTP Digits:")
        num=int(input())
        for r in range(num):
            l=random.randint(0,7)
```

```
num=int(input())
for r in range(num):
    l=random.randint(0,7)
    p=random.randint(0,7)
    q.append(matrix[1][p])
    print("DYNAMIC OTP IS:-")
    for k in q:
        print(k," ",end="")
    print("\n to continue Generating Passwords Press 0 Else Press 1")
    ch=int(input())
    if(ch==0):
        flag=0
    elif(ch==1):
        flag=1

print(q)
o="".join([str(elem) for elem in q])
mainOTP = o
url = pyqrcode.create(o)
url.svg("OTP.svg", scale = 20)
cairosvg.svg2png(url="OTP.svg", write_to="OTP.png")
#url.png('OTP.png')

#-----Code for SKIN OTP STARTS HERE-----#

mat=[]
a=[x for x in range(65,91)]
for f in range(48,58):
    a.append(f)
for e in range(97,123):
    a.append(e)
a.append(35)
a.append(42)
matrix=[]
for i in range(0,8):
    inArray=[]
    for j in range(0,8):
        c=random.randint(0,len(a)-1)
        a.remove(c)
        inArray.append(chr(c))
        matrix.append(inArray)
    for r in range(num):
        l=random.randint(0,7)
        p=random.randint(0,7)
        mat.append(matrix[1][p])
    print("SKIN OTP IS:-")
    for k in mat:
        print(k," ",end="")
    print("\n")
m="".join([str(elem) for elem in mat])
skinOTP = m
url1 = pyqrcode.create(m)
url1.svg("SKINOTP.svg", scale = 20)
cairosvg.svg2png(url="SKINOTP.svg", write_to="SKINOTP.png")
#url1.png('SKINOTP.png')

org = cv2.imread('OTP.png', cv2.IMREAD_UNCHANGED)
fil = cv2.imread('SKINOTP.png', cv2.IMREAD_UNCHANGED)
b1a = cv2.addWeighted(org,0.5,fil,0.5,0)
```

```
#-----Code for SKIN OTP STARTS HERE-----#

mat=[]
a=[x for x in range(65,91)]
for f in range(48,58):
    a.append(f)
for e in range(97,123):
    a.append(e)
a.append(35)
a.append(42)
matrix=[]
for i in range(0,8):
    inArray=[]
    for j in range(0,8):
        c=random.randint(0,len(a)-1)
        a.remove(c)
        inArray.append(chr(c))
        matrix.append(inArray)
    for r in range(num):
        l=random.randint(0,7)
        p=random.randint(0,7)
        mat.append(matrix[1][p])
    print("SKIN OTP IS:-")
    for k in mat:
        print(k," ",end="")
    print("\n")
m="".join([str(elem) for elem in mat])
skinOTP = m
url1 = pyqrcode.create(m)
url1.svg("SKINOTP.svg", scale = 20)
cairosvg.svg2png(url="SKINOTP.svg", write_to="SKINOTP.png")
#url1.png('SKINOTP.png')

org = cv2.imread('OTP.png', cv2.IMREAD_UNCHANGED)
fil = cv2.imread('SKINOTP.png', cv2.IMREAD_UNCHANGED)
b1a = cv2.addWeighted(org,0.5,fil,0.5,0)
```



```
Meet - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C/Aadi/index.html x +
https://colab.research.google.com/drive/13alPH5I6C0eHC2sWlOX78/a5v0O2iDC#scrollTo=vNXVg4oexCs
NIS_PROJECT.ipynb
File Edit View Insert Runtime Tools Help
RAM Disk
Editing
Files
gdrive
sample_data
OTP.png
OTPSvg
SKINOTP.png
SKINOTPSvg
Transmission_OTP.png
+ Code + Text
[10] bld = cv2.addWeighted(org,0.5,fil,0.5,0)

Enter The Number of OTP Digits:
6
DYNAMIC OTP IS:-
D F 1 X S 3
To Continue Generating Passwords Press 0 Else Press 1
1
['D', 'F', '1', 'X', 'S', '3']
SKIN OTP IS:-
h k E f p Z 5

print(mainOTP)
DF1XS3

#-----Transmission OTP for HTTP Protocol Transmission-----#
# Client Side

cv2.imwrite('Transmission_OTP.png', bld)
org = cv2.addWeighted(bld,2,fil,-1, 0)

[5] from google.colab import drive
drive.mount('/content/gdrive')

Mounted at /content/gdrive

[7] #-----Program on the END USER to Retrieve OTP-----#
org = cv2.addWeighted(bld,2,fil,-1, 0)
cv2.imwrite('Retrieved_OTP.png', org)

0s completed at 6:30 PM
```

```
Meet - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C/Aadi/index.html x +
https://colab.research.google.com/drive/13alPH5I6C0eHC2sWlOX78/a5v0O2iDC#scrollTo=vNXVg4oexCs
NIS_PROJECT.ipynb
File Edit View Insert Runtime Tools Help Saving...
RAM Disk
Editing
Files
gdrive
sample_data
OTP.png
OTPSvg
SKINOTP.png
SKINOTPSvg
Transmission_OTP.png
+ Code + Text
[10] DYNAMIC OTP IS:-
D F 1 X S 3
To Continue Generating Passwords Press 0 Else Press 1
1
['D', 'F', '1', 'X', 'S', '3']
SKIN OTP IS:-
h k E f p Z 5

print(mainOTP)
DF1XS3

[6] #-----Transmission OTP for HTTP Protocol Transmission-----#
# Client Side

cv2.imwrite('Transmission_OTP.png', bld)
org = cv2.addWeighted(bld,2,fil,-1, 0)

[5] from google.colab import drive
drive.mount('/content/gdrive')

Mounted at /content/gdrive

[7] #-----Program on the END USER to Retrieve OTP-----#
org = cv2.addWeighted(bld,2,fil,-1, 0)
cv2.imwrite('Retrieved_OTP.png', org)

True

0s completed at 6:30 PM
```

```
Meet - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C/Aadi/index.html x +
https://colab.research.google.com/drive/13alPH5I6C0eHC2sWlOX78/a5v0O2iDC#scrollTo=vNXVg4oexCs
NIS_PROJECT.ipynb
File Edit View Insert Runtime Tools Help All changes saved
RAM Disk
Editing
Files
gdrive
sample_data
OTP.png
OTPSvg
SKINOTP.png
SKINOTPSvg
Transmission_OTP.png
+ Code + Text
[10] Enter The Number of
6
DYNAMIC OTP IS:-
D F 1 X S 3
To Continue Genera
1
['D', 'F', '1', 'X',
SKIN OTP IS:-
h k E f p Z 5

print(mainOTP)
DF1XS3


[6] #-----Transmission OTP for HTTP Protocol Transmission-----#
# Client Side

cv2.imwrite('Trans
org = cv2.addWeigh

[5] from google.colab
drive.mount('/cont

Mounted at /conten

[7] #-----Program on the END USER to Retrieve OTP-----#
org = cv2.addWeigh
cv2.imwrite('Retri

OTP.png x


0s completed at 6:30 PM
```

Meer - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C:/Aadi/index.html x +

https://colab.research.google.com/drive/13alPH5I6C0e6HC2sWlOX787a5v0O2rDC#scrollTo=vHXVg40aeCs

NIS_PROJECT.ipynb ☆

File Edit View Insert Runtime Tools Help All changes saved

You are sharing your entire screen. Stop Sharing

Comment Share Settings

RAM Disk

Editing

Files

- gdrive
- sample_data
- OTP.png
- OTP.svg
- SKINOTP.png
- SKINOTP.svg
- Transmission_OTP.png

Code + Text

```
[10] Enter The Number of
6
DYNAMIC OTP IS:-
D F 1 x s 3
To Continue Generat
1
['D', 'F', '1', 'x
SKIN OTP IS:-
h k e f p z

print(mainOTP)
DF1xs3


[6] #-----
# Client Side

cv2.imwrite('Trans
org = cv2.addweigh

[5] from google.colab
drive.mount('/cont
Mounted at /content

[7] #-----
org = cv2.addweigh
cv2.imwrite('Retri
```

SKINOTP.png



Meer - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C:/Aadi/index.html x +

https://colab.research.google.com/drive/13alPH5I6C0e6HC2sWlOX787a5v0O2rDC#scrollTo=vHXVg40aeCs

NIS_PROJECT.ipynb ☆

File Edit View Insert Runtime Tools Help All changes saved

You are sharing your entire screen. Stop Sharing

Comment Share Settings

RAM Disk

Editing

Files

- gdrive
- sample_data
- OTP.png
- OTP.svg
- SKINOTP.png
- SKINOTP.svg
- Transmission_OTP.png

Code + Text

```
[10] Enter The Number of
6
DYNAMIC OTP IS:-
D F 1 x s 3
To Continue Generat
1
['D', 'F', '1', 'x
SKIN OTP IS:-
h k e f p z

print(mainOTP)
DF1xs3


[6] #-----
# Client Side

cv2.imwrite('Trans
org = cv2.addweigh

[5] from google.colab
drive.mount('/cont
Mounted at /content

[7] #-----
org = cv2.addweigh
cv2.imwrite('Retri
```


Transmission_OTP.png



Meer - dti-qubi-gfa x WhatsApp x NIS_PROJECT.ipynb - Colaboratory x /C:/Aadi/index.html x +

file:///C:/Aadi/index.html

You are sharing your entire screen. Stop Sharing



Success

We received your purchase request;
we'll be in touch shortly!

Conclusion

In conclusion, there have been numerous approaches to dealing with the issue of OTPs being leaked as well as other security concerns. In today's world, they are the most widely used means of authentication. Our solution, which uses QR code technology on top of that while simultaneously employing the same technology to safeguard the data, is efficient and dependable, making it a very easy decision for users or organisations. This approach can be utilised in a variety of applications, including authentication, message transfer within a specified range, and so on. Finally, this project improved the existing architecture to make it far more resistant to attacks while maintaining the same degree of user accessibility.

Future Work

Enhanced Authentication scheme using Dynamic Password (EDAP) method can be used to link a Windows application to a database or an external embedded system device, such as a folder locker or an external gateway authentication. This authentication mechanism is not utilized in any Internet banking application in India. As a result, banks can use this authentication system to enhance their security. Aside from that, the EADP scheme can be used to store secret data in military companies and in any other application where security is paramount. The EADP can generate passwords with "n" characters, so it can be used to encrypt highly important information and improve security in the field of information technology.

References

1. https://en.wikipedia.org/wiki/QR_code
2. <https://blog.bio-key.com/dynamic-password-enforcing-authentication-otp>
3. Figure-1. https://en.wikipedia.org/wiki/File:QR_code_for_mobile_English_Wikipedia.svg3. M. H. S. AbouSteit, A. F. Tammam and A. Wahdan, "A Novel Approach For Generating One-Time Password With Secure Distribution," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 461-466, doi: 10.1109/WorldS450073.2020.9210322.
4. D. Pansa and T. Chomsiri, "Dynamic Password Authentication: Designing step and security analysis," 2012 7th International Conference on Computing and Convergence Technology (ICCT), 2012, pp. 518-523.
5. M. Shakir and A. A. Khan, "S3TFPAS: Scalable shoulder surfing resistant textual-formula base password authentication system," 2010 3rd International Conference on Computer Science and Information Technology, 2010, pp. 12-14, doi: 10.1109/ICCSIT.2010.5564479.
6. G. S. K. Fung, R. W. H. Lau and J. N. K. Liu, "A signature based password authentication method," 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation, 1997, pp. 631-636 vol.1, doi: 10.1109/ICSMC.1997.625824.
7. D. Pansa and T. Chomsiri, "Integrating the Dynamic Password Authentication with Possession Factor and CAPTCHA," 2018 Joint 10th International Conference on Soft Computing and Intelligent Systems (SCIS) and 19th International Symposium on Advanced Intelligent Systems (ISIS), 2018, pp. 530-535, doi: 10.1109/SCIS-ISIS.2018.00093.
8. Cambou, Bertrand, David Hély, and Sareh Assiri. "Cryptography with analog scheme using memristors." *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 16, no. 4 (2020): 1-30.
9. Vassena, Marco, Craig Disselkoen, Klaus von Gleissenthall, Sunjay Cauligi, Rami Gökhan Kıcı, Ranjit Jhala, Dean Tullsen, and Deian Stefan. "Automatically eliminating speculative leaks from cryptographic code with blade." *Proceedings of the ACM on Programming Languages* 5, no. POPL (2021): 1-30.
10. Zeng, Jianhua, Yanlin Zhan, and Jianrong Yang. "Encryption and Decryption of Optical Images with Different Algorithms." In *Proceedings of the 2nd International Conference on Artificial Intelligence and Advanced Manufacture*, pp. 256-265. 2020.
11. Malik, Muhammad Wito, Diyanatul Husna, I. Ketut Eddy Purnama, Ingrid Nurtanio, Afif Nurul Hidayati, and Anak Agung Putri Ratna. "Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method." In *2020 the 6th International Conference on Communication and Information Processing*, pp. 153-158. 2020.

12. [Gong, Bo-fan. "Hybrid Compression and Lightweight Encryption of Color Image."In Proceedings of the 2020 5th International Conference on Multimedia Systems and Signal Processing, pp. 36-39. 2020.](#)
13. [M. Karnan and N. Krishnaraj, "Bio password — Keystroke dynamic approach to secure mobile devices," 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010, pp. 1-4, doi: 10.1109/ICCIC.2010.5705901.](#)
14. [Yi-Pin Liao, Shuenn-Shyang Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces, Volume 31, Issue 1,2009, Pages 24-29, ISSN 0920-5489, <https://doi.org/10.1016/j.csi.2007.10.007>. \(<https://www.sciencedirect.com/science/article/pii/S0920548907001043>\)](#)
15. [Kurogi T., Yamaba H., Aburada K., Katayama T., Park M., Okazaki N. \(2018\) A Study on a User Identification Method Using Dynamic Time Warping to Realize an Authentication System by s-EMG. In: Barolli L., Xhafa F., Javaid N., Spaho E., Kolici V. \(eds\) Advances in Internet, Data & Web Technologies. EIDWT 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 17. Springer, Cham. \[https://doi.org/10.1007/978-3-319-75928-9_82\]\(https://doi.org/10.1007/978-3-319-75928-9_82\)](#)
16. [Alpar O., Krejcar O. \(2015\) Pattern Password Authentication Based on Touching Location. In: Jackowski K., Burduk R., Walkowiak K., Wozniak M., Yin H. \(eds\) Intelligent Data Engineering and Automated Learning – IDEAL 2015. IDEAL 2015. Lecture Notes in Computer Science, vol 9375. Springer, Cham. \[https://doi.org/10.1007/978-3-319-24834-9_46\]\(https://doi.org/10.1007/978-3-319-24834-9_46\)](#)
17. [X. Liu, T. Huang, X. Wang and X. Tang, "A user authentication scheme based on dynamic password for wireless sensor networks," 2010 International Conference on Intelligent Computing and Integrated Systems, 2010, pp. 145-148, doi: 10.1109/ICISS.2010.5656792.](#)
18. [Velásquez, Ignacio & Caro, Angelica & Rodríguez, Alfonso. \(2017\). Authentication Schemes and Methods: a Systematic Literature Review. Information and Software Technology. 94.10.1016/j.infsof.2017.09.012.](#)
19. [Yohan Muliono, Hanry Ham, Dion Darmawan, 2018, Keystroke Dynamic Classification using Machine Learning for Password Authorization, Procedia Computer Science 135 \(2018\) 564–569](#)
20. [Geng B., Ge L., Wang Q., Wang L. \(2018\) Improved Digital Password Authentication Method for Android System. In: Huang DS., Jo KH., Zhang XL. \(eds\) Intelligent Computing Theories and Application. ICIC 2018. Lecture Notes in Computer Science, vol 10955. Springer, Cham. \[https://doi.org/10.1007/978-3-319-95933-7_86\]\(https://doi.org/10.1007/978-3-319-95933-7_86\)](#)
21. [Orcan Alpar,Intelligent biometric pattern password authentication systems for touchscreens, Expert Systems with Applications, Volume 42, Issues 17–18, 2015, Pages 6286-6294, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2015.04.052>. \(<https://www.sciencedirect.com/science/article/pii/S0957417415002948>\)](#)
22. [Pin Shen Teh, Andrew Beng Jin Teoh, Connie Tee, Thian Song Ong, Keystroke dynamics in password authentication enhancement, Expert Systems with Applications, Volume 37, Issue](#)

12, 2010, Pages 8618-8627, ISSN 0957-4174,

<https://doi.org/10.1016/j.eswa.2010.06.097>. (<https://www.sciencedirect.com/science/article/pii/S0957417410006019>)

23. [C. Wang and C. Feng, "Security Analysis and Improvement for Kerberos Based on Dynamic Password and Diffie-Hellman Algorithm," 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013, pp. 256-260, doi: 10.1109/EIDWT.2013.49.](#)
24. [Aaron L.-F. Han, Derek F. Wong, Lidia S. Chao, 2020, Advances of Password Cracking and Countermeasures in Computer Security, NLP2CT Lab, University of Macau, Macau SAR ILLC, University of Amsterdam, Science Park 107, 1098 XG Amsterdam](#)
25. [J. Weaver, K. Mock and B. Hoanca, "Gaze-based password authentication through automatic clustering of gaze points," 2011 IEEE International Conference on Systems, Man, and Cybernetics, 2011, pp. 2749-2754, doi: 10.1109/ICSMC.2011.6084072.](#)
26. [Andriotis P., Tryfonas T., Oikonomou G. \(2014\) Complexity Metrics and User Strength Perceptions of the Pattern-Lock Graphical Authentication Method. In: Tryfonas T., Askoxylakis I. \(eds\) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Cham. \[https://doi.org/10.1007/978-3-319-07620-1_11\]\(https://doi.org/10.1007/978-3-319-07620-1_11\)](#)
27. [L. Wu, T. Chen, C. Qiao and Z. Li, "Authentication Technology of Mobile Internet of Things Based on the Dynamic Password," 2018 IEEE International Conference of Safety Produce Informatization \(IICSPI\), 2018, pp. 204-208, doi: 10.1109/IICSPI.2018.8690463.](#)
28. [Kapil Juneja, An XML transformed method to improve effectiveness of graphical password authentication, Journal of King Saud University - Computer and Information Sciences, Volume 32, Issue 1, 2020, Pages 11-23, ISSN 1319-1578, <https://doi.org/10.1016/j.jksuci.2017.07.002>. \(<https://www.sciencedirect.com/science/article/pii/S131915781730112X>\)](#)
29. [M. Martinez-Diaz, J. Fierrez and J. Galbally, "Graphical Password-Based User Authentication With Free-Form Doodles," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 4, pp. 607-614, Aug. 2016, doi: 10.1109/THMS.2015.2504101.](#)
30. [Fan C., Bai C., Zou J., Zhang X., Rao L. \(2015\) A Dynamic Password Authentication System Based on NoSQL and RDBMS Combination. In: Zhang R., Zhang Z., Liu K., Zhang J. \(eds\) LISS 2013. Springer, Berlin, Heidelberg. \[https://doi.org/10.1007/978-3-642-40660-7_121\]\(https://doi.org/10.1007/978-3-642-40660-7_121\)](#)
31. [Deng K., Zhang Y. \(2012\) Dynamic Password Authentication Protocol Using Interference Factor. In: Qian Z., Cao L., Su W., Wang T., Yang H. \(eds\) Recent Advances in Computer Science and Information Engineering. Lecture Notes in Electrical Engineering, vol 127. Springer, Berlin, Heidelberg. \[https://doi.org/10.1007/978-3-642-25769-8_87\]\(https://doi.org/10.1007/978-3-642-25769-8_87\)](#)
32. [Kiss P.J., Klimkó G. \(2020\) Authentication of Electronic Legal Statements by a Trust Service Provider Using Two-Factor Dynamic Handwritten Signature Verification. In: Kő A., Francesconi E., Kotsis G., Tjoa A., Khalil I. \(eds\) Electronic Government and the Information](#)

Systems Perspective. EGOVIS 2020. Lecture Notes in Computer Science, vol 12394. Springer, Cham. https://doi.org/10.1007/978-3-030-58957-8_11

33. https://www.researchgate.net/publication/345417526_Securing_password_using_dynamic_password_policy_generator_algorithm
34. https://www.researchgate.net/publication/216813107_Applying_QR_code_in_augmented_reality_applications
35. https://www.researchgate.net/publication/254056851_oPass_A_User_Authentication_Protocol_Resistant_to_Password_Stealing_and_Password_Reuse_Attacks
36. Sutheebanjard, P. & Premchaiswadi, Wichian. (2010). QR-code generator. 89-92. 10.1109/ICTKE.2010.5692920.
Link: https://www.researchgate.net/publication/251987247_QR-code_generator
37. Tiwari, Sumit. (2016). An Introduction to QR Code Technology. 39-44. 10.1109/ICIT.2016.021.
Link: https://www.researchgate.net/publication/318125149_An_Introduction_to_QR_Code_Technology
38. Ugwu, CHIDIEBERE & Mesigo, T. (2015). A Novel Mobile Wallet Based on Android OS and Quick Response Code Technology. International Journal of Advanced Research in Computer Science and Technology. 3. 85.
Link: https://www.researchgate.net/publication/277014768_A_Novel_Mobile_Wallet_Based_on_Android_OS_and_Quick_Response_Code_Technology
39. Abhishek Mehta, Dr. Kamini Solanki 2021 Design and Development of QR Code Recognition from Digital Image international Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181
Link: <https://www.ijert.org/research/design-and-development-of-qr-code-recognition-from-digital-image-IJERTCONV9IS05039.pdf>
40. Divya Sharma, Volume 2, Issue 2, February – 2017 A Review of QR code Structure for Encryption and Decryption Process International Journal of Innovative Science and Research Technology
ISSN No: - 2456- 2165
Link: <https://ijisrt.com/wp-content/uploads/2017/03/A-Review-of-QR-code-Structure-for-Encryption-and-Decryption-Process.pdf>
41. Kuan-Chieh Liao, Wei-Hsun Lee, Min-Hsuan Sung, Ting-Ching Lin
A One-Time Password Scheme with QR-Code Based on Mobile Phone
https://www.researchgate.net/publication/221521693_A_One-Time_Password_Scheme_with_QR-Code_Based_on_Mobile_Phone
42. Abey Abraham; Alina Poly; T Aishwarya; Anju George
SPAQ: Secure PIN authentication using QR code
<https://ieeexplore.ieee.org.egateway.vit.ac.in/document/8250661?arnumber=8250661>

43. [Yaoqiu Hong](#)
[Design of Intelligent Access Control System Based on DES Encrypted QR Code](#)
<https://ieeexplore.ieee.org.egateway.vit.ac.in/document/9213475/authors#authors>
44. [Mete Eminagaoglu; Ece Cini; Gizem Sert; Derya Zor](#)
[A Two-Factor Authentication System with QR Codes for Web and Mobile Applications](#)
<https://ieeexplore.ieee.org.egateway.vit.ac.in/document/6982784>
45. [Jisha Thomas; R.H Goudar](#)
[Multilevel Authentication using QR code based watermarking with mobile OTP and Hadamard transformation](#)
<https://ieeexplore.ieee.org.egateway.vit.ac.in/document/8554891>
46. https://www.researchgate.net/publication/261388669_Dynamic_Password_Authentication_Designing_step_and_security_analysis
47. <https://dl.acm.org/doi/10.1145/1971519.1971593>