Plagiarism Checker X Originality Report

Similarity Found: 21%

Date: Monday, February 21, 2022
Statistics: 746 words Plagiarized / 3518 Total words
Remarks: Medium Plagiarism Detected - Your Document needs Selective Improvement.

Image Based Encryption System Abstract In today's world of modernization and the web, client confirmation and security have been the foremost imperative need in many organizations and companies. There's a considerable inquiry within the field of information privacy. Unfortunately, the strategies of putting away and covering up touchy data like passwords and personal data have fizzled to fetch enough consideration from the analysts. Within the last decade, a parcel of analysts recommended the utilization of a combination of security strategies like steganography and cryptography to elevate the security of the framework.

In any case, it still does not guarantee sufficient information security. In this paper, we propose a framework that executes numerous encryption strategies with a decentralized and distributed capacity of delicate data of clients and offers multi-layered security to the system. In this plan, we scramble the information utilizing AES-128, split it into pieces, and stow away it behind the pictures utilizing steganography utilizing AES-128 adding another layer of encryption and storing it Introduction: Every single day the innovation is progressing in any case, the secret word remains unaltered as the most well-known way of client confirmation. To get to any private and 'secure' framework a user needs to go through a client confirmation preparation.

The client confirmation handle can involve the confirmation of one or more of a few information (like a secret word), something in possession (like an RFID get to card), or inherence (just like the unique mark) of the substance. Over the past few a long time, the essential cruel of client authentication has been the passwords within the shape of the text. Users enroll on the frameworks by putting a username and watchword to log in to the framework and gain get to it. The client is anticipated to keep in mind this mystery data to pass the user authentication preparation. Considering the number of client accounts individuals have these days on social media, work-related emails, drives, websites, etc.

it might be exceptionally troublesome for the user to keep in mind all those passwords. At that point, clients tend to utilize the same watchword for different systems putting its security at stake and after that comes to RFID access cards and biometric user authentication within the picture, which are one of a kind. But at the conclusion of the day, the address arises on the security of the watchword capacity.

No matter what rules have been taken after to create an in a perfect world secure secret word, the address remains the same, is it being put away on a secure system in a secure manner? Different frameworks store passwords in their database in their claim fashion. It moreover depends on the type of database framework being utilized. Having private data put away at the centralized database framework has demonstrated to be exceedingly unreliable from time to time. In any case, putting away this confidential data in a conveyed way makes it troublesome for the aggressor to track it down to every single area and perform the assault.

The support and security of the password record within the database is still a point of concern in different areas. Numerous websites are not following the great capacity hone which would in a perfect world incorporate encryption, great hashing algorithms, salting, and a large number of rounds. In the past, numerous famous organizations like Yahoo, LinkedIn, Joined together Countries, and Sony Online Amusement were assaulted for ignoring these security measures.

Touchy commerce data is at the chance when it falls into the hands of unauthorized individuals with malevolent eagerly. Considering the simple availability of hacking tables and instruments on the web, to hinder the essential level of security with attacks such as Lexicon assault, Rainbow table assault, Crossover assault, Brute drive assault and Smart brute constrain assault it is exceptionally troublesome for this security degree to guard the framework against such assaults when they are considered to be secure. It would be a botch to depend on these measures totally expecting that the framework is unbreakable.

Too, looking at the advanced hacking procedures trending within the advertise these days, white cap programmers are coming up with innovative arrangements to ensure the system against them. To extend the security of the systems and keep the information exchange secure all through the web, different strategies have been designed such as Advanced Watermarking, Cryptography, and Steganography. Be that as it may, the attackers are effectively being able to enter the framework in a few or the other way.

Subsequently, it has become exceptionally vital for the security analysts and experts to come up with a stronger solution that's inflexible sufficient to be entered and adaptable sufficient to be suited in varied environments. The arrangement must be something that mixes the existing security arrangements and enhances the security indeed more. It is conceivable with multi-layered security implementation using the decentralized watchword capacity system. This inquires about rotates around a combined technique that blends these security techniques with regard to the edge cryptography framework. Performing the combination of steganography and cryptography ensures a tall level of information security.

Literature Survey We can classify passwords as the most important and crucial resource being stored in the database. Hence, in the past extensive research has been done and a lot of researchers from around the world have published their research about its security, attacks on the database system, password attacks, innovative ways of performing those attacks and defense systems against them. Some recommended the use of images or separate use of steganography and cryptography for user authentication, while some suggested the combination of steganography and cryptography for the same.

Considering the fact that each one of them had some strengths and weaknesses that sometimes they significantly shielded the system or failed due to some gaps in their method of implementation. 2.1. Image authentication In [6] the authors proposed an image-based authentication system with the use of steganography. Highlighting the issues with current authentication systems such as, having to remember the alphanumeric passwords and people having a number of user accounts on the internet they accidentally or lazily set the same password for multiple user accounts which is a potential security threat. They suggest an innovative system where the password is hidden behind a secret image using steganography and stored in the database.

At the time of sign up, a traditional process is followed but the user is also asked to browse and provide a secret image that has the password embedded in it. The user details with the password embedded secret image stored in the server database. Next time the user logs in, the login interface sends the username in plaintext and the secret image is sent in the bit stream. They argue that in case the password and the secret image is known to the attacker, it would still be impossible for them to penetrate through the system as the database not only compares the images and the passwords but also the dimensions of the image [6]. However, in [7] a unique way has been introduced for user authentication. In their exceptional way of authentication, they used a clickbased graphical password scheme which is a cued-recall graphical password technique.

Basing their research on Passpoint [8], which was proposed in 2005, where the password was composed of numerous points anywhere on the image. They also suggested a "robust discretization" system with a variety of conflicting grids enabling login attempts to be recognized that strongly resembled with the correct form and translating the password inserted into a key for cryptographic authentication. Hence, CCP proposed an alternative way to it using the hotspot technique. Rather than clicking on multiple points on a single image, the user has to click on one point on each image as there would be multiple images to be clicked by the user.

The authors conclude by arguing that the CCP is securer than the graphical authentication methods that have been introduced previously. Resulting in which, it makes it difficult for the attackers to acquire the correct sets of images for the user and then analyze the correct hotspots on each of those images [7]. 2.2. Steganography and cryptography In the past, a lot of researchers have directed their research towards the combination of two or more security measures. Therefore, steganography and cryptography have been the most relied one by them.

Considering the fact, that steganography itself applies cryptography while hiding the text behind. Hence, [9] explain the way of using steganography and encryption to make the data secure. They suggest that Elliptic Curve Cryptography can be used for image encryption Huffman Coding method for image steganography, and Discrete Wavelet Transform for image compression. In their work, they argue that the Elliptic Curve Cryptosystem is the most secure one out of all the existing cryptosystems.

Most importantly by comparing the Elliptic Curve Cryptosystem with Diffie-Hellman or RSA, they highlight that it provides the same level of security with much shorter keys. Provided that, it offers higher speeds, lesser power consumption, bandwidth savings, and storage efficiencies. This could particularly be useful where processing capacity, bandwidths, power availability or storage are required [9]. As well as in [10] the researchers are using the combination of security measures like steganography and cryptography to make the system secure.

But with a different method as they proposed a blend of steganography with the use of discrete cosine transform (DCT) and cryptography using the one-time pad or vernam cipher implemented on a digital image and measuring the quality of the image using the peak signal to noise ratio (PSNR) and the quality of the extraction of the decrypted message using Normalized Cross Correlation (NCC). They proposed an embedding algorithm to perform this operation. The results were measured in Peak Signal to Noise Ratio (PSNR) and Mean square error (MSE). The smaller value of the MSE depicted the better quality of the output image. In the final result, the average value of the MSE was 0.50232 which proved to be a reliable way of implementing a combination of cryptography and steganography. Also, they suggested that encryption methods such as AES, RSA, and DES could be considered to be combined with steganography in future [10].

Few researchers tried to go one step ahead and use the renowned and stronger encryption algorithms as they are considered, such as AES and RSA. While few tried to modify the existing one or combine them with other algorithms like SHA512 and MD5. According to [11] integrating AES and RSA together and applying steganography elevates the security of the system. In their research, they propose a combined and alternative approach to secure the system using cryptography and steganography. They used two encryption algorithms, AES (with symmetric keys) and RSA (with asymmetric keys) with image steganography.

To justify their choice, they mention that combining these three techniques together helps to construct a strong communication system based on steganography that can sustain several types of cyberattacks, reverse engineering and detection systems. The entire operation has three main components: sending, transmitting and receiving. The sender uses three inputs for the communication, secret data to be transmitted, cover image to hide the secret data and the public RSA key of the receiving party. By using the private RSA key, the steganographic image, receiver decrypts the secret data. Their system used AES-128 for primary encryption.

With each new communication string, the encryption key (128 bits) is formed and consists of two parts: calculated and random, both being128-bit in size. a pseudo-random pattern generator (PRPG) seeded with either variable or constant data is used to generate the 1st half of the AES Key which is a random part of the key. Non-volatile color information (NVCI) is used to calculate the computed part of the encryption key which is the 2nd half of the AES Key.

Using a powerful algorithm such as SHA512, MD5, the high order bits of each color channel (RGB in a color image) are hashed. Also, it needs to be noted that only half of the hash value is used in the 2nd half of the AES key. The data is embedded in the image using the data rearrangement method and LSB pixel mapping. The steganographic image travels through any communication channel like email, network, file sharing, etc. and in the end, the receiver's system processes the VCI part of the steganographic image to decrypt it. The receiver's system recovers the 1st and the 2nds half of the AES key.

In the end, the receiver decrypts the intended secret data after retrieving both the halves of the AES key [11]. Research done in [12] also introduced the same combined approach to ensure the security of the data by merging steganography and cryptography using the AES-128 algorithm but they also modified the existing AES algorithm. They mentioned that security operations take place in parts to achieve two levels of security.

In the two parts of their research, in the first part, they modified the AES algorithm to accommodate the steganography method that they implemented, and it is called AES_MPK algorithm and in the second part, the same AES_MPK algorithm is merged with the steganography algorithm to hide the encrypted secret behind the image. To perform the first part of the operations, the authors required the output in the form of MPK digits as MSLDIPMPK and PVD_MPK methods use the MPK digits for hiding the data. Hence, the revised AES algorithm was called AES_MPK algorithm. And in the second part, they encrypted the message M using AES_MPK algorithm using the key K and produce the ciphertext.

Later the same ciphertext is hidden behind the cover image C using the MSLDIP-MPK and PVD_MPK methods to produce the steganographic image S. They conclude that with the implementation of their proposed method it would be easier to transmit the data even over the open channels as the ciphertext would not fetch the unwanted attention as it is hidden behind the image and it is capable of hiding a large amount of information than existing methods. Also, their system provides two layers of security making the system even more secure [12]. 2.3.

Evaluation of cryptography algorithms While giving attention to the multi-layered and decentralized security measure, it is very crucial to choose the method that is more reliable and flexible. Some researchers have written papers where they have compared and evaluated the existing cryptography algorithms. Like in [13] an evaluation operation was performed to compare the top encryption algorithms, the authors compared these algorithms with respect to the encryption, decryption and packet size.

Referring to the results shown below in figure 1, they concluded that AES is much better than RSA and DES. S.no _Algorithm _Packet Size (KB) _Encryption time(sec) _Decryption time(sec) _ _1. _AES _153 _1.6 _1 _ _ _DES _153 _3.0 _1.1 _ _ _RSA _153 _7.3 _4.9 _ _2. _AES _868 _2.0 _1.8 _ _ _DES _868 _4.0 _1.2 _ _ _RSA _868 _8.2 _5.1 _ _ Methodology The execution of the proposed investigation was separated into 3 stages- encryption and encoding, steganography, and unscrambling. Within the to begin with stage, the secret word was scrambled utilizing AES-256 and encoded in Base64 i.e. different of 4, as we part the secret word into 4 pieces.

In stage II we performed steganography by covering up the scrambled pieces of watchword behind the pictures by implementing another lever of AES-256 encryption. Within the last stage III, we recovered the password by unscrambling the pieces of the secret word and combining them within the redress arrangement. Concurring to the examination worn out the writing audit, it is evident that keeping the delicate data at the decentralized area by executing a more grounded encryption calculation like AES-128 and combining it with other security strategies like steganography upraises the security of the system.

Consequently, the inquiry about centers on the security of the capacity framework by bringing in the attention towards the way in which the touchy data is put away, encryption, image steganography, and secret word part strategy. Conclusion The most objective of this inquiry was to decide on the off chance that the security of the framework can be enhanced by combining the security strategies such as steganography, encryption, and splitting the secret information which is the watchword in our case. Moreover, by doing this, we needed to test whether putting away private information in a decentralized design makes a difference to progress security.

Referring to the comes about that we have gotten by actualizing the proposed arrangement on various platforms, we conclude that the arrangement is profoundly versatile as Python programming is cross-platform. In expansion, executing multi-layered encryption with the utilize of stronger encryption strategies like AES-256 boosts the trouble level for the programmers to penetrate through the system. Varied working frameworks don't directly affect the execution of our solution strategy which suggests actualizing this arrangement and performing the operation on tall resolution pictures the least setup required for the framework is 8GB ram with a faster processor like i5 or above. the execution of the framework was great on the Linux working framework as compared to the Mac working system. Hence, machines with higher arrangements are profoundly suggested to progress the performance of the proposed solution.

References [1] V. Venukumar and V. Pathari, “Multi-factor authentication using threshold cryptography,” in 2016 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Jaipur, India, Sept 21-24, 2016. [2] M. M. Kassim and A. S. , “ProcurePass: A user authentication protocol to resist password stealing and password reuse attack,” in 2013 International Symposium on Computational and Business Intelligence, New Delhi, India, 2013. [3] D. Mirante and J.

Cappos, “Understanding password database compromises,” 2013. [Online]. Available: https://pdfs.semanticscholar.org/0337/d1329f79b8b736295d9c056b012faf7343c4.pdf. [Accessed 3 Dec 2019]. [4] E. S. I.

Harba, “Advanced password authentication protection by hybrid cryptography & audio steganography,” Iraqi Journal of Science, vol. 59, no. 1C, pp. 600-606, 2018. [5] J. H. Kennedy, M. T. A. Khan, M. J. Ahmed and M. Rasool, “Image steganography based on AES algorithm with huffman coding,” International Journal of Engineering Science and Computing, April 2017, vol. 7, no. 4, pp. 6352-6355, 2017. [6] S. K. Sonker, S. Kumar, A. Kumar and D. P. Singh, “Image based authentication using steganography technique,” International Journal of Advanced Research in Computer Science, vol. 4, no. 8, pp. 277-282, May/June 2013. [7] V. Moraskar, S. Jaikalyani, M. Saiyyed, J. Gurnani and K.

Pendke, “Cued Click Point technique for graphical password authentication,” International Journal of Computer Science and Mobile Computing, vol. 3, no. 1, pp. 166-172, January 2014. [8] S. Wiedenbeck, J. Watersa, J.-C. Birget, A. Brodskiy and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of HumanComputer Studies, vol. 63, no. 1-2, pp. 102-127, July 2005. [9] L. Sharma and A. Gupta, “Image encryption using Huffman Coding for steganography,,” International Journal of Advance research , Ideas and Innovations in Technology, vol. 2, no. 5, pp. 1-10, 2016. [10] D. R. I. M. Setiadi, E. H. Rachmawanto2 and C. A.

Sari, “Secure image steganography algorithm based on DCT,” Journal of Applied Intelligent System, vol. 2, no. 1, pp. 1-11, April 2017. [11] S. F. Mare, M. Vladutiu and L. Prodan, “Secret data communication system using steganography, AES and RSA,” in 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME), Timisoara, Romania, October 20-23, 2011. [12] M. E. Saleh, A. A. Aly and F. A. Omara, “Data security using cryptography and steganography techniques,” (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, pp. 390-397, 2016. [13] P. Mahajan and A.

Sachdeva , “A study of encryption algorithms AES, DES and RSA for security,” Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 15, pp. 15-21, 2013. [14] P. Patil, P. Narayankar and S. M. Meena, “A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish,” in International Conference on Information Security & Privacy (ICISP2015), Nagpur, India, December 2015. [15] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979. [16] RSA, “RSA Distributed Credential Protection,” RSA-EMC2, London, 2012. [17] G. I. Davida, D. J. Linton, C. R. Szelag and D. L.

Wells, “Database security,” IEEE Transactions on Software Engineering, Vols. SE-4, no. 6, pp. 531 - 533, Nov. 1978. [18] S. Imran and I. Hyder, “Security issues in databases,” in 2nd International Conference on Future Information Technology and Management Engineering, Sanya, China, 13-14 Dec. 2009. [19] G. Singh and Supriya, “A study of sncryption slgorithms (RSA, DES, 3DES and AES) for information security,” International Journal of Computer Applications, vol. 67, no. 19, pp. 33- 38, April 2013. [20] G. Singh, A. Singla and K. S.

Sandha, “Cryptography algorithm comparison for security enhancement in wireless intrusion detection system,” International Journal of Multidisciplinary Research, vol. 1, no. 4, pp. 143-151, August 2011. [21] OWASP, “OWASP SecList Project,” 7 November 2018. [Online]. Available: https://www.owasp.org/index.php/OWASP_SecLists_Project. [Accessed 10 June 2019]. [22] csafe, “Stego App DB,” 04 April 2019. [Online]. Available: https://data.csafe.iastate.edu/StegoDatabase/. [Accessed 15 July 2019]. [23] B. A. Meier, Python GUI Programming Cookbook - Second Edition, Birmingham, UK: Packt Publishing, May 2017.

INTERNET SOURCES:

<1% - https://www.bnpevents.com/webinars/security
<1% - https://www.usenix.org/conference/usenixsecurity21/technical-sessions
<1% - https://giallone.blogspot.com/2017/06/oath2.html
<1% - https://speakerdeck.com/romaness/hbr-strategy-articles
<1% - https://silo.pub/snakes-in-suits-when-psychopaths-go-to-work.html
<1% - https://www.onlineessayhelp.net/
13% - http://norma.ncirl.ie/4168/1/nilishabwandile.pdf
<1% -
https://www.researchgate.net/publication/221174270_An_Image_Encryption_and_Authentication_Scheme
<1% -
https://www.researchgate.net/publication/308732797_Secure_and_Authentic_DCT_Image_Steganography_through_DWT_-_SVD_Based_Digital_Watermarking_with_RSA_Encryption
1% -
https://www.academia.edu/71064855/Secure_Image_Steganography_Algorithm_Based_on_DCT_with_OTP_Encryption
<1% -

https://www.researchgate.net/publication/342239219_Image_Segmentation_Algorithms_for_Banana_Leaf_Disease_Diagnosis

<1% - https://www.spamtitan.com/web-filtering/page/2/

<1% - https://www.researchgate.net/publication/49591261_On_the_Differences_between_Hiding_Information_and_Cryptography_Techniques_An_Overview

1% - https://www.researchgate.net/profile/Lucian-Prodan/publication/254011793_Secret_data_communication_system_using_steganography_AES_and_RSA/links/561e375108aec7945a25436a/Secret-data-communication-system-using-steganography-AES-and-RSA

<1% - https://www.mdpi.com/1424-8220/22/3/1109/html

<1% - http://www.edu.dhsphn.tbmc.edu.vn/cRrjohxF_information-hiding-using-steganography-welcome-to_Pw.pdf

<1% - https://dokumen.pub/introduction-to-modern-cryptography-3rd-edition-0815354363-9780815354369-1351133039-9781351133036-1351133012-9781351133012-1351133020-9781351133029-1351133004-9781351133005.html

<1% - https://www.sciencedirect.com/science/article/pii/S0166361517304244

<1% - https://researchr.org/publication/icacci-2016

<1% - https://www.researchgate.net/publication/325264071_Advanced_Password_Authentication_Protection_by_Hybrid_Cryptography_Audio_Steganography

<1% - https://www.ijcsi.org/papers/IJCSI-8-5-2-145-154.pdf

<1% - https://www.ijert.org/high-end-secure-image-transfer-using-vector-quantization

1% - https://www.slideshare.net/irjetjournal/irjet-study-and-performance-evaluation-of-different-symmetric-key-cryptography-technique-for-encryption

<1% - http://pen.ius.edu.ba/index.php/pen/article/view/1092

1% - https://jtsiskom.undip.ac.id/index.php/jtsiskom/article/view/13468

1% - https://link.springer.com/chapter/10.1007/978-981-15-7907-3_39

<1% - https://dl.acm.org/doi/book/10.5555/539308

1% - https://www.hindawi.com/journals/tswj/2013/704865/

1% - https://www.coursehero.com/file/68770828/Integrating-AES-DES-and-3-DES-Encryption-Algorithms-for-Enhanced-Data-Securitypdf/

<1% - http://jasa-cari-buku.com/knowledgebase.php?article=1675