JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Novel Concept Of XOR Based Encrypted Image And Setagno Data Transfer

Shalini[1], Prof. (Dr.) Saroj Hiranwal[2]

M.Tech Research Scholar[1], Principal RIET Campus, Jaipur (PhD in Computing Science)[2]

[1,2]Electronics & Communication Engineering Department (VLSI)

Rajasthan institute of engineering and technology (RIET), Jaipur, Rajasthan, India

Abstract : Security is always a major concern in this field. Thus, for the safe transmission of information including pictures, encryption methods are consistently sought and there should always be a need for better strategies to be developed and implemented to give greater security. Security also plays a significant role in protecting assets from unapproved access. Digital images are a popular choice for passwords because they're easy to remember, fun to share, and give you peace of mind. Use images instead of words as an important element of your security system. This will help you make sure you know that all the assets in your system are safe. The proposed work is using encrypted images as authentication, combined with hashing algorithms like SHA-512 or MD5. These algorithms generate secure passwords by combining the image and data file; it also offers steganographic ways to securely share information.

IndexTerms **– Encrypted Image , Data Security**

I. INTRODUCTION

The process of safeguarding digital data throughout its entire life cycle to prevent corruption, theft, or unauthorized access is known as data security. Hardware, software, storage devices, and user devices are all included. Administrative controls and access; and the procedures and policies of organizations. Data security makes use of technologies and tools that make it easier to see what is being done with a company's data and how it is used. Through processes like data masking, encryption, and sensitive information redaction, these tools can safeguard data. Additionally, the procedure aids businesses in streamlining their auditing procedures and adhering to the increasingly stringent regulations pertaining to data protection. An organization can safeguard its data from cyberattacks thanks to a robust data security management and strategy process. Additionally, it assists them in reducing the threat of insider threats and human error, which continue to be the root cause of numerous data breaches. [1] Data security is important to businesses in all sectors worldwide for a variety of reasons. Customers' and users' data must be safeguarded from loss or theft so that it does not fall into the wrong hands. Organizations are required by law to safeguard data in accordance with industry and state regulations like the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS). [2]

Cybersecurity for data is also important for avoiding the reputational risk that comes with a data breach. Customers may move their business to a competitor as a result of a well-publicized hack or data loss. In the event that sensitive data is lost, this also runs the risk of significant financial losses, as well as payments for legal fees, damages, and fines. [2] Data security is a way of securing data to avoid any chance of a breach, which could cause sensitive information to be exposed. For example, a data security policy may dictate that only designated employees or contractors are allowed to access customer payment data--no exceptions. [3]

Data privacy, on the other hand, is about strategic decisions about what information to share with people. If a development team says "it might be valuable for us to know how many customers have been paying via PayPal so that we can decide if it's worth accepting Stripe, Payoneer and Skrill as well," they might suggest that you share customer payment data with them for the next two weeks. [3]

II. LITERATURE SURVEY

A. I. Shaban and N. Haryani Zakaria[4] The current trend toward graphical passwords for protecting customers' personal data has necessitated additional efforts to improve their security features. In this paper, we show how a graphical secret phrase is built based on the social knowledge of images that customers have in the Malaysian context. In order to identify the commonality angle in relation to social foundation, a control-research center investigation with 30 members was conducted. The obtained results showed that the majority of members at least include one recognizable image in their graphical secret phrase choices. The findings may suggest that one of the factors that has a significant impact on customers' secret word decisions is social foundation.

P. Chithra and K. Sathya[5] describe PixCaptcha as a graphical secret word that is completed by editing the chosen image in accordance with the clues and gluing it in the appropriate location. The scrambled graphical secret word's information base is broken by the programmer with the Rainbow table attack, despite the fact that graphical passwords are the best replacement for alpha numeric passwords. Rainbow tables break secret words much faster than previous methods like animal power breaking and word reference attacks. Before the secret word is saved in the database, a solid encryption calculation is used in this case. The Gaussian Elimination Technique is used, and Cleaves encryption is another encryption scheme that provides solid resistance to attacks from Rainbow tables.

A. Mukerjee et al.[6] This paper revolves around changing the course of action of having 'text' as mystery key as people will overall consistently neglect to recall their passwords and have to recover it. Proposing the arrangement of using a picture as a secret phrase that is stored encrypted in a database and can be decoded and coordinated to see if the client approves. Experiments have shown that a person's mind remembers an image, something they can see, more easily than text.

F. Z. Glory et al.[7] Everybody who uses a variety of web-based services is concerned about the safety and security of protecting personal data from hackers. The password authentication framework is one of many available authentication frameworks for protecting individuals' information. Password security and legitimacy have become fundamental and essential topics as a result of the growth of web advocacy, electronic trade, data movement, and data sharing. However, it is also required to guarantee the password's strength. As a result, complex password designs are suggested by all digital specialists. In any case, in light of those perplexing examples, users frequently forget their passwords. In contrast to other erroneous password generators, authors propose a novel calculation in this paper that will generate a secure password.

III. PROPOSED WORK

Enrolling User

Stage 1: Input User Name

Stage 2: Select the Image which to be encrypted to be used as password

Step3: Select the Hash algorithm SHA or MD5 which is to be used for the generation of thehash code on the basis of the select image.

Step 4: Set PASSCODE=HASH (1:20), where HASH is the hash generated on the basis ofthe SHA or MD5 algorithm selected by user.

Stage 5: Encrypt the Image using the Key generated on the basis of Dimensions of Image andusing XOR encryption encrypt the image.

Step 6: Store all the details like user name, encrypted image path, PASSCODE and otherdetails in the table for the registered user.

Step 7: STOP

Validating Users

Step 1: Read Username and PASSCODE.

Step 2: Fetch the Encrypted Image from Database.

Step 3: Decrypt the image.

Step 3: If Details verified in Database,
thenGrant Access
Else:

Print "Invalid Login Details"[End of if Structure]

Step4: End

IV. PROPOSED WORK

The implementation is performed using the MATLAB and MS ACCESS database.

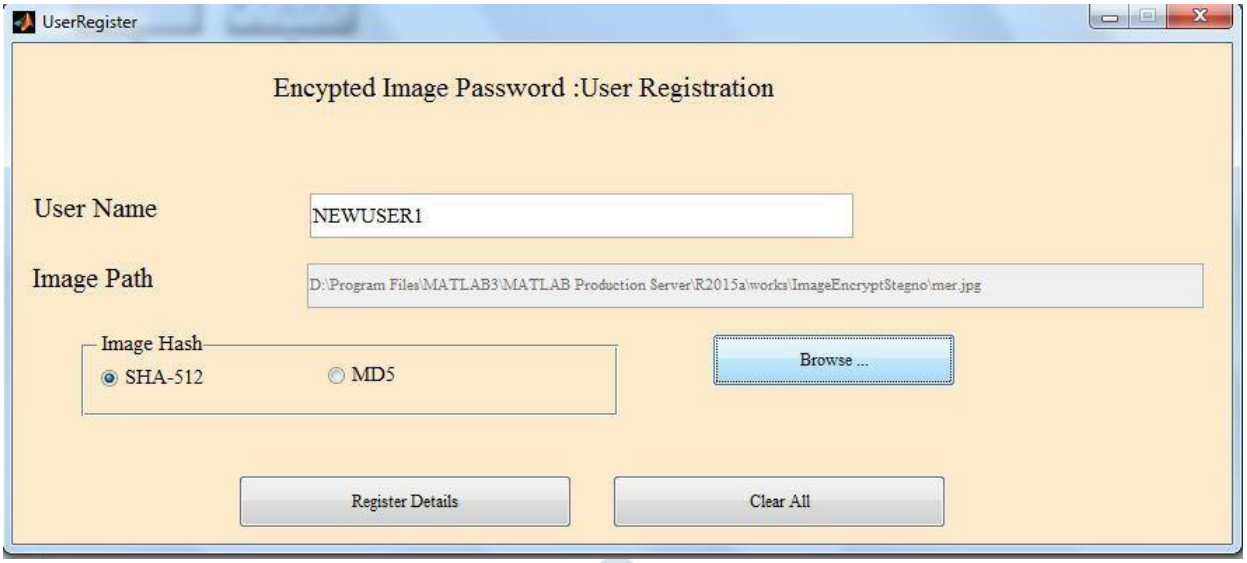

Fig 1. Implementation Snap Shot

TABLE 1 BASE PAPER RESULT (Farhana Zaman Glory et. Al 2019)

OTP	Website/Tool	Result
{urBn17iRfan- 1	Rumkin	71.6 bits Entropy
{urBn17iRfan- 1	Password Blue zxcvbn	49 bits
{urBn17iRfan- 1	Cryptool2	Bit Strength 92

TABLE 2 PROPOSED WORK RESULTS

OTP	Website/Tool	Result
12940972653082271991-@-1124707475587489795 8-#->	Rumkin	146.1 bits Entropy
12940972653082271991-@-1124707475587489795 8-#->	Password Blue zxcvbn	144 bits
12940972653082271991-@-1124707475587489795 8-#->	Cryptool2	Bit Strength 110

V. ACKNOWLEDGMENT

In the correspondence, security is always a major concern. Encryption methods will always be sought after for the secure transmission of any information, including images, and there will always be a need for better strategies to be developed to provide greater security. As a result, asset security is also a significant responsibility of security. So, pictures as a mystery word is the improved substitute for ensuring about the resources and there similarly the better estimations will reliably expect for making access more ensured about. Although only image passwords can be cracked, encrypted image passwords are quite challenging to break. The idea of using encrypted images as passwords is very useful for authenticating users. The steganographic method of data sharing is proposed, in which the data is hidden in the original image using the combination key that is generated using the original image file and data file, and the encrypted image is used as authentication in conjunction with using the SHA-512 or MD5 hash algorithms that generate the PASCODE using the image. The shared data are made more secure and secure thanks to the cross-validation concepts.

REFERENCES

1. S. Jain and A. Khunteta, "Color Image Encryption by Component Based Partial Random Phase Encoding," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, pp. 144-148.
2. Ramaraju, P. V., G. Nagaraju, and R. K. Chaitanya. "Image Encryption and Decryption using Advanced Encryption Algorithm." The International Daily journal. Discovery Publication, 2015.
3. L. Gunaseeli and R. A. Canessane, "Graphical passwords implies on tolerance password, image choice, and puzzle login security," 2017 International Conference on Information Communication and Embedded Systems (ICICES), 2017, pp. 1-8.

4. Shaban, A. I. , & Haryani Zakaria , N. (2018), The Impact Of Cultural Familiarity On Choosing Image For Recognition-Based Graphical Passwords, International Conference on Computer and Information Sciences (ICCOINS).
5. Pl, Chithra & Sathya, Sathya K. (2019). Pristine PixCaptcha as Graphical Password for Secure eBanking using Gaussian Elimination and Cleaves Algorithm.
6. A. Mukerjee, S. Som, S. K. Khatri and A. Mathur, "Enhancing Remembrance of Password as an Image," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 198-203.
7. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2019, pp. 0416-0423
8. Chaudhari, Savita B. Hajare, Poonam S. Bhusare E & TC,& Pune University Maharashtra, India , 2015
9. Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. 2010. The security of modern password expiration: an algorithmic framework and empirical analysis. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, 176–186.
10. Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. 2010. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). Association for Computing Machinery, New York, NY, USA, 162–175.
11. Ross, Steven A., et al. “Sketcha: A Captcha Based on Line Drawings of 3D Models.” Jhalderm.com, https://jhalderm.com/pub/papers/sketcha-www10.pdf, 2010.
12. Payne, Bryan & Edwards, W.. (2008). A Brief Introduction to Usable Security. Internet Computing, IEEE. 12. 13-21. 10.1109/MIC.2008.50.