Design and Implementation of Visual Cryptography Application for University Result System

S.K.Patil[1], S.A.Badarkhe[2], Pratik Mandlik[3], Sanskruti Nimbalkar[4], Sushil Pabale[5]

Department of E&TC, SKNCOE, SPPU, Pune

[1]skpatil_skncoe@sinhgad.edu,
[2]smita.garde_skncoe@sinhgad.edu,
[3]pratikmandlik2@gmail.com
[4]sanskrutinimbalkar141@gmail.com
[5]sushilpabale07@gmail.com

Abstract-*The new area of research is image cryptography. There are numerous cryptography techniques that have been developed. In order to conceal the visual details (images, text, etc.) in images, many encryption techniques have been used. The primary principle of encryption is the probability of human vision decryption if the right key image is used, known as visual cryptography. Using visual cryptography and digital watermarking, a new method for user authentication is suggested.Using visual cryptography and digital watermarking; a user authentication method is suggested. The original picture, mainly the approved person's photograph, is split into shares. One of the shares is kept within the server and the other is sent by mail to the approved person. When the share is downloaded and submitted to the web by the authorized person, two sections are combined and the user receives a single captcha image containing the password after entering which user can login to the system.*

Keywords- *Secured University results, visual cryptography, JSP, servlet, java, web*

I. INTRODUCTION

The existing paper used by universities uses a centralized system of databases that stores all their data in one location. Hence, when it comes to defense, this system is not that trustworthy. To ensure that only approved participants can access the system, the system used in our project utilizes visual cryptography. In addition, data is stored in various databases, ensuring data confidentiality. Data stored in databases is stored in encrypted form which adds extra dimension to security. The existing system used by universities uses a centralized system of databases that stores all their data in one location.The same unified database is accessed by all the actors involved in the system. As everybody accesses the same database, this is the key downside, so improvements made to this database go unnoticed. Without adding any encryption, the current device stores data as it is.The current system receives input from the student, the examiner and the supervisor, and all changes, enhancements and data are applied to a single database. The architecture used is very simple and basic. Different forms of potential risks, such as data theft, data modification, etc., are not considered. The current infrastructure is vulnerable to multiple attacks. Therefore, to make it more reliable, the system needs to be updated. We will implement visual cryptography for examiner login for authentication purposes.

II. LITERATURE SURVEY

In the paper, “Advantages and disadvantages of using cryptography in steganography” [1] present two steganography algorithms, so that one cryptographic algorithm will be used to encrypt the message before the steganography operation. In the following, the advantages of using and not using these cryptographic algorithms against its disadvantages are reviewed and suggestions about their use in steganography algorithms and systems are presented.

From the paper, “Implementation and Analysis of Various Visual Cryptographic Techniques for Sensitive Data Protection” author has given visual cryptography is the cryptographic technique in which various forms of visual data like pictures, texts, etc. are encrypted such that they cannot be directly read and need to be visually decrypted for use. Sensitive data like defense data involves diverse content types and different formats of data related to criminology, military, aeronautics, communications and space flights. Communicating the crucial data safely is a topic of vital concern for government. This paper intends to analyze the various cryptographic techniques and explore appropriate visual cryptographic solution for securing the sensitive data.

The paper, “Improving Quality of Friendly Progressive Visual Secret Sharing using Essential Shares” implements FPVSS using essential shares to overcome the problems of existing work. In addition to that, the proposed scheme can also be used in hierarchy secret sharing. The simulation result shows the effectiveness of proposed scheme.

A Paper titled, “Analysis of Feature Enhancements in Visual Secret Sharing”, analyzes the feature advancements in the VSS field. The VSS approaches remain distinct from the conventional cryptography, thereby offering new security solutions in many applications. Security being the central and challenging demand in contemporary information systems, the analysis of the state-of-the-art VSS stands significant.

The paper, “On the Analysis and Design of Visual Cryptography with Error Correcting Capability” investigates a VCS with t-error correcting capability (VCS-tEC). To the best of our knowledge, VCS-tEC is introduced for the first time. Three (k, n)-VCS-tEC schemes are proposed: the separated scheme, the integrated scheme, and the nonsystematic scheme.

III. METHODOLOGY

The original picture will be split into shares at the time the user logs in. One of the shares is kept within the server and the other is sent by mail to the examiner. When the share is downloaded by the approved individual and submitted to the web, two sections are combined and the user receives a single captcha image containing the password after entering which user can login to the system.

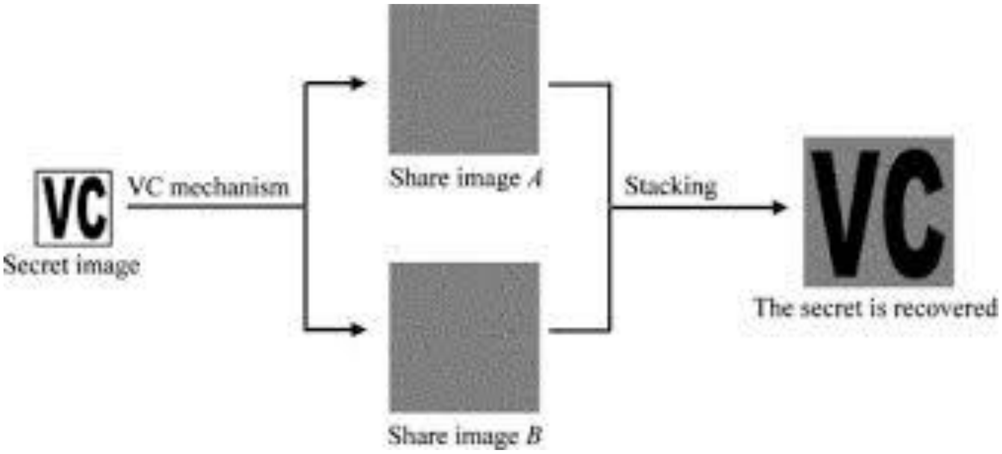

Fig. 1 Modified system architecture for university result system

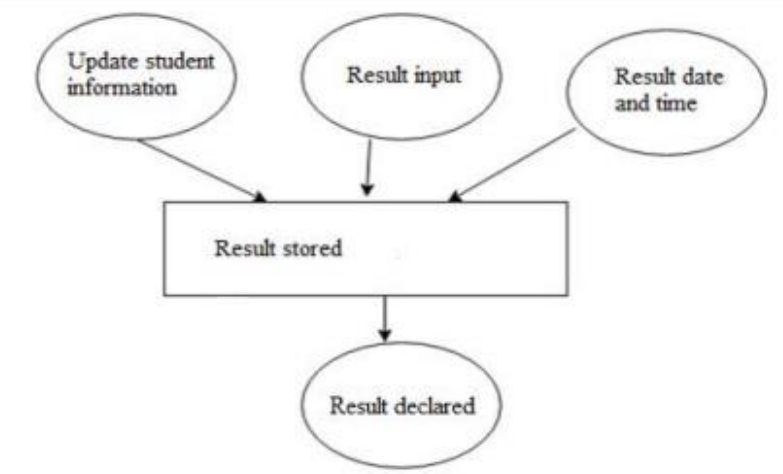

Fig. 2 Input output scenario of University result system

This system takes input from student, examiner or admin in various forms such as updating student information, entering student marks, entering results information, etc. The output of the system is result of students.

CONCLUSION

This paper aims to introduce a framework to handle results safely and transparently by implementing cryptographic functionality. By designing, analyzing and testing the architecture that helps to overcome the limitations of previous work, the outlined result framework will be created. We will demonstrate that cryptography gives universities a new opportunity to switch from a centralized scheme to a more efficient database scheme, while growing the current scheme's security measures and providing new options for transparency. Moreover to this, various security measures including visual cryptography and encryption are introduced to make system more stable. To create Captcha, visual cryptography combines two pictures. One picture is sent to the email of the examiner, and another is generated by the server. In this way, visual cryptography guarantees that the device can only be accessed by certified examiners. Data would be stored in encrypted form in databases, which renders it incapable of reading even though anyone accesses the device.

REFERENCES

[1] Ali Hadipour; Raheleh Afifi, “Advantages and disadvantages of using cryptography in steganography” 2020 17th International ISC Conference on Information Security and Cryptology (ISCISC).

[2] N. Jeyanthi, Somya Brijesh Shastri, Prashasti Baranwal, R Thandeeswaran, Akash, “Implementation and Analysis of Various Visual Cryptographic Techniques for Sensitive Data Protection” 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)

[3] Srividhya Sridhar; Gnanou Florence Sudha, “Improving Quality of Friendly Progressive Visual Secret Sharing using Essential Shares” International Conference on Communication and Signal Processing (ICCSP)

[4] Raviraja Holla M.; D. Suma, “Analysis of Feature Enhancements in Visual Secret Sharing”, 2020 International Conference on Communication and Signal Processing (ICCSP)

[5] Ching-Nung Yang; Yi-Yun Yang, “On the Analysis and Design of Visual Cryptography with Error Correcting Capability” IEEE Transactions on Circuits and Systems for Video Technology (Early Access)

[6] Yi Liu and Qi Wang “An Database management based on Blockchain” International Conference on Applied System Innovation 2018.

[7] Bin Duan, Ying Zhong, IEEE Member, Dayu Liu:- Institute of Electrics, Chinese Academy of Sciences Beijing, China “Education application of blockchain technology :learning outcome and meta-diploma” IEEE 23rd International Conference on Parallel and Distributed Systems ICPADS.2017.00114 2017.

[8] Eli Ben Sasson ; Alessandro Chiesa ; Christina Garman ; Matthew Green ; Ian Miers ; Eran Tromer ; Madars Virza, “Zerocash: Decentralized Anonymous Payments from Bitcoin” IEEE Symposium on Security and Privacy, IEEE. SP.2014.36 2014

[9] Sachchidanand Singh- IBM Software Lab., Nirmala Singh- Tech Mahindra “Blockchain: Future of Financial and Cyber Security” 2nd International Conference on Contemporary Computing and Informatics 2016.

[10] LIJING ZHOU , LICHENG WANG , YIRU SUN, AND PIN LV State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China Corresponding author: Licheng Wang “BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation” National Key Research and Development Program, China ACCESS.2018.2847632, 2018.

[11] Jiin-Chiou Cheng１, Narn-Yih Lee2, Chien Chi3, and Yi-Hua Chen4 1,2,3Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan, Taiwan “Blockchain and Smart Contract for Digital Certificate” Proceedings of IEEE International Conference on Applied System Innovation IEEE ICASI 2018- Meen, Prior & Lam 2018.