iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Student Authentication Framework for Online Examination using Visual Cryptography

Ms.Vaishali B.Bhagat

[#]*Deaprtment Of Computer Science and Engineering, RTMNU*

Abstract*— In the recent years, internet has become increasingly popular and used by many people from all over the world. Online learning is widely acceptable. Online examination is a fundamental part of online learning. Student work and assessment is remotely submitted without any face to face interaction. Student may submit already submitted work so originality of material is greatly defeated. Therefore Student authentication in online examination is seen as a one of the major problem and challenges. This paper proposed the novel student authentication framework for online examination. Visual cryptography is used to make system more secure and reliable. The proposed system also ensures genuine interaction of individual students with the online examination and also verifies the identity of online student.

***Keywords*— Visual Cryptography, Share, Stego image, Visual Secret sharing Scheme**

I. INTRODUCTION

Today's world is a internet world. Many people from all over the world uses the internet to transmit their confidential information over the communication network.Nowdys online learning has become increasingly popular. Online examination play very vital role in online education. Online education material is easily accessible and widely updatable. Hence various educational institute, banking sector adopt this in large scale. In the online examination scenario, there is no face to face interaction between students and system administrators. Thus security has become important issue in this scenario. During online examination, students submit their work remotely. So it becomes difficult to verify the identity of person taking online examination. Students may submit plagiarize work as part of their assessment. Student imitates or uses the original work of other author. so plagiarism can be one of the major challenges to online learning. Online learning offer more opportunities for cheating and academic dishonesty in such examination. Cheating in online examination seems to be very serious issue. So there is necessity of more reliable and secure student authentication system. This paper provide more secure authentication framework for online examination using visual cryptography and try to overcome all the problems occurs during examination. The proposed method uses visual cryptography to generate shares and these shares are encrypted separately using RSA algorithm to provide more security to shares. One share is kept at server database and other is sent by email to students. Students have to upload share at the time of examination. Both shares are stacked together to reveal original image.Authneticity of students is verified if both shares are matched otherwise students is not allowed to access the examination link. and also report the system administrator about the fraud.

II. VISUAL CRYPTOGRAPHY

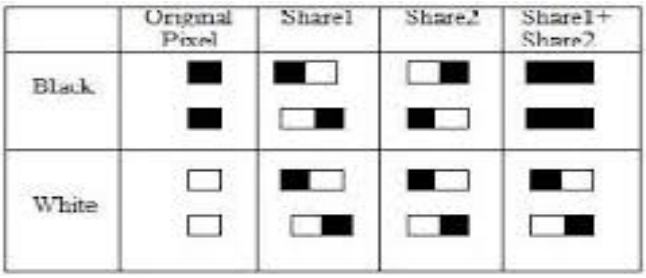
Visual cryptography is cryptographic technique which allow visual information to be encrypted in such way that decryption can be performed by human visual system. It is visual secret sharing scheme, where image is broken into number of shares and all the shares are printed separately on transparencies. Single share does not reveal the information .Decryption can be performed by stacking all shares together to produce original image. Various visual secret sharing schemes are available to provide more secure image transmission over the network. The basic model of visual cryptography proposed by Naor and Shamir accepts a binary image 'I' as the secret image, and divides it into 'n' number of shares. Each pixel of image 'I' is represented by 'm' sub pixels in each of the 'n' shared images. Stacking of shares reveals the secret image but increases the size by 'm' times. The various black and white visual cryptography schemes can be summarized as follows:

1) 2 out of 2 scheme*:* In this, the secret image is distribute on two shares which are both required for the decryption process. This is depicted in Figure 1.This scheme can be realized by using either 2 sub pixels or 4 sub pixels to

ISSN: 2321-9653

represent each pixel of the secret image as explained below.

2 sub pixels: Each pixel is subdivided into one black and ne transparent (white) sub pixel as shown in



4 sub pixels: Each pixel is subdivided into four sub pixels, two black and two transparent (white)

2) n out of n scheme*:* In an n out of n scheme the secret message is distributed on n transparencies. Superimposing I transparencies with i < n will not reveal any information of the secret image. There exist two possible ways to construct an n out of n scheme by using 2n sub pixels or 2n-1 sub pixels.

3) k out of n scheme: Splitting of the secret message into n shares out of which any k shares are required for decryption. Contrary to the n out of n scheme, not all n transparencies are required for the decryption in this case k < n.In 1996, Ateniese, Blundo, & Stinson [2] proposed extended visual cryptography schemes in which shares contain not only the secret information but are also meaningful images

III. AUTHENTICATION METHODS

There are various authentication methods are developed to verify authenticity of users. They are Knowledge-Based, Object-Based, Biometic-Based, Profile Based Authentication methods. They are mainly based on user's knowledge, objects and biometric features and profiles.

Knowledge-Based Authentication Method:-It verifies the identity of students based on personal knowledge. Students provide login credential to access online examination portal. Students may share their credential to third party to improve their grades and marks.

Object-Based Authentication Method:-In this method, Students need to provide physical object i.e electronic chip,cards,magnetic cards, digital key to prove their identity .In electronic cards identification features of students are stored. At the time of online examination, both entities are required. Attacker may theft these cards and pretends as authorized user and uses the services of portals.

Biometric-based Authentication Method: - In recent years biometric based authentication system become more popular and many organizations adopt this to prevent fraud. Biometric based system store the different physical features of people into their database in template form. Attacker may alter this template. If Biometric template is modified by attacker then authenticate user may not able to access resources.

Profile-Based Authentication Method: - In this method, user-id, password and challenge questions are used for student authentication during online examination. Attacker may hack or crash student profile database. If student profile database is crashed or hacked by intruder then authorized student may not able to appear for online examination.

All this methods have their own limitation and advantages. Main goal of these methods to develop student authentication more reliable and secure. In a current scenario, most of the organizations and education institute, Banking sector uses this technique to conduct online examination. To remove all the shortcoming occurs in the above technique, I proposed the student authentication framework to conduct the examination more smoothly and securely.

IV.PROPOSED METHOD

STUDENT AUTHENTICATION FRAMEWORK USING VISUAL CRYPTOGRAPHY

In this framework, multilayer authentication approach is used. The solution consist of multiple phases to produce reliable authentication framework.i.e.Registration phase ,share creation and generation phase, share encryption phase, Online examination phase, Share decryption phase and finally Authentication phase. Initially students collect login-id and password by entering all personal and academic detail into online server and also upload their photo and signature into it. During share creation phase, student signature image and photo image are taken together to produce stego image and this stego image is then store in original host image and then generate the shares. All the shares are encrypted before given to student by email. The primary focus of proposed solution to secure student authentication for online examinations. When student upload his share during authentication process, software on server side, stack the shares together (one at client side and other at server side) to reveal the host image. In this method, for encryption and decryption of shares, RSA algorithm is used to make approach more secure. In the proposed method visual cryptography technique is applied to student authentication system. Single share does not reveal any information. Hence it provides more security to system.

ISSN: 2321-9653

V. PHASES OF PROPOSED SYSTEM

A. ***Registration Phase:***-The student those who want to apply for online exams, visit the exam website. And complete the registration form by filling the personal and academic details. The students also upload their scanned photo and signature image onto server. In the last stage of this phase, student have to choose the cover image form the set of images provided by server portal and finally student click on the submit button to complete the registration process successfully.

B. ***Share Creation and Generation Phase:***-After the completion of registration phase, students were notified by email to login and access examination link. Actually before this, software at server site generate the share by hiding stego image into original host image that was selected by student at the time of registration.Stego image consist of photo image which consist of signature image and then shares are generated .

C. ***Share Encryption Phase:***-Shares are encrypted separately using RSA algorithm and share1 is sent by email to students.RSA algorithms is one of the popular encryption algorithms. Server uses his private key to encrypt the share.

D. ***Online Examination Phase:-***In this phase, user log-in to examination portal by entering id and password onto portal .User were ask to complete the authorization process where user have to upload their share which is sent by mail.

E. ***Share Decryption Phase:***-Software on server side collect the share, one from student and other from server database where share is stored in encrypted form, decrypt it using server public key separately. Now this two shares are overlapped together to original host image.Stego image is now reveal from host image using other algorithm. Photo image and signature images are revealed from stego image.

F. ***Authentication Phase:-***In this phase, reconstructed photo image and signature image are matched with original images stored in server database at the time registration. If match found, student is granted access to online examination otherwise student access is blocked and reported to system administrator.

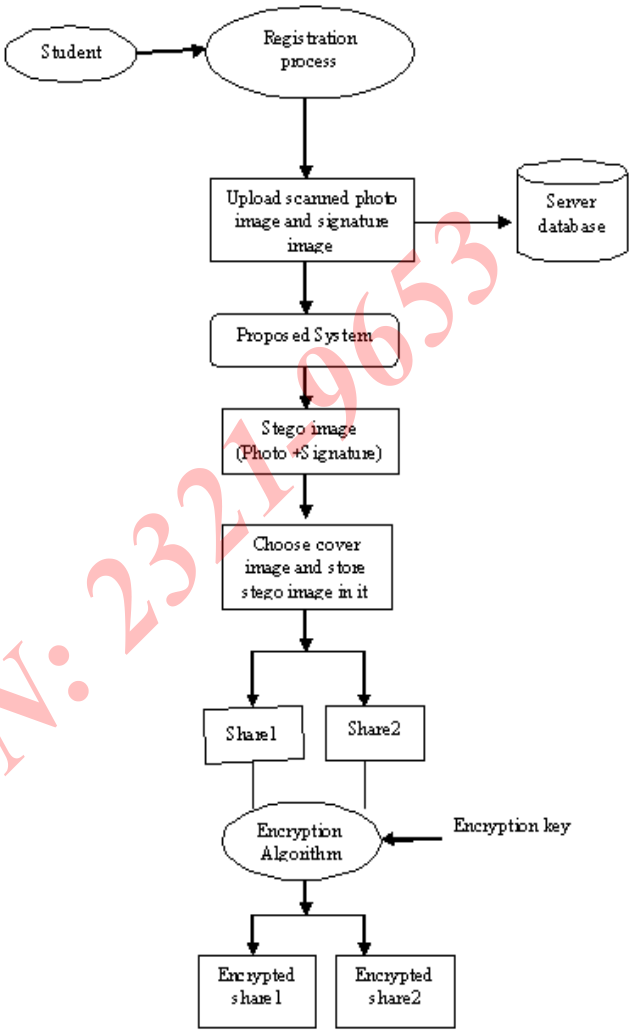


Fig2. Encryption at server side

In above diagram, operation in registration process is presented. Students upload scanned photo and signature image at the time of registration. Signature image is hided in photo image and this image is called stego image. Students also choose one of the cover image and store stego image into it.two shares are generated using visual cryptography and encrypted using RSA algorithm. One encrypted share is sent by email to students and other is kept at server side.

ISSN: 2321-9653

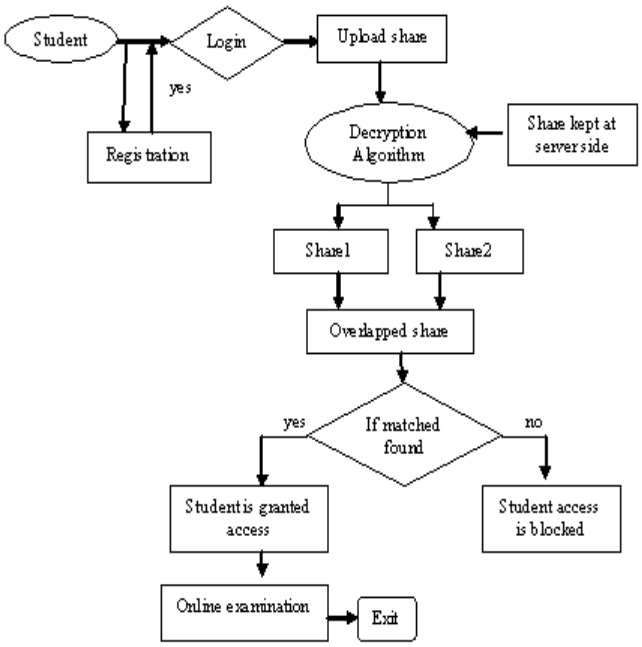


Fig2.Proposed Model

In the above diagram, proposed model is presented.When students enter their log-in id and password to system,online examination portal is opened where students upload the share and server send its corresponding share .Both share are decrypted using same algorithms.By stacking both share together ,Original host image is established.Stego image is recovered from it It also verify the authenticity of student and allow them to continue otherwise fraud is detected and access is blocked for that students.

VI. Conclusions

The proposed system provides more secure student authentication system for online examination using three layer of security. First layer provide user-id and password to student who apply for online examination by email. so only those students have log-in id and password are allowed to appear for examination. Second layer generate the shares of stego image, so student have to upload the one share and only genuine user can provide this share. Otherwise access is not granted to them, in this way more security is provided by system. Third layer provide security to shares also, so no advertiser can not alter it's bit sequence and not able to create fake shares. The proposed system is specially developed to prevent fraud in online examination.

References

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[2] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson,"Extended Visual Capabilities for Visual Cryptography,"Theoretical Computer Science, vol.250, pp.143-161, 2001

[3] Adamski M., Saeed K. "Online Signature Classification and its Verification System", 7th Computer Information Systems and Industrial Management Applications2008, p.

[4] Aggarwal G., Ratha N., Jea T. Y., Bolle R. "Gradientbased Textural Characterization of Fingerprints",Biometrics: Theory, Applications and Systems, 2008,IEEE.

[5] Agulla E. G., Rifón L. A., Castro J. L. A., Mateo C. G."Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments", Eighth IEEE International Conference on Advanced Learning Technologies, 2008, IEEE.

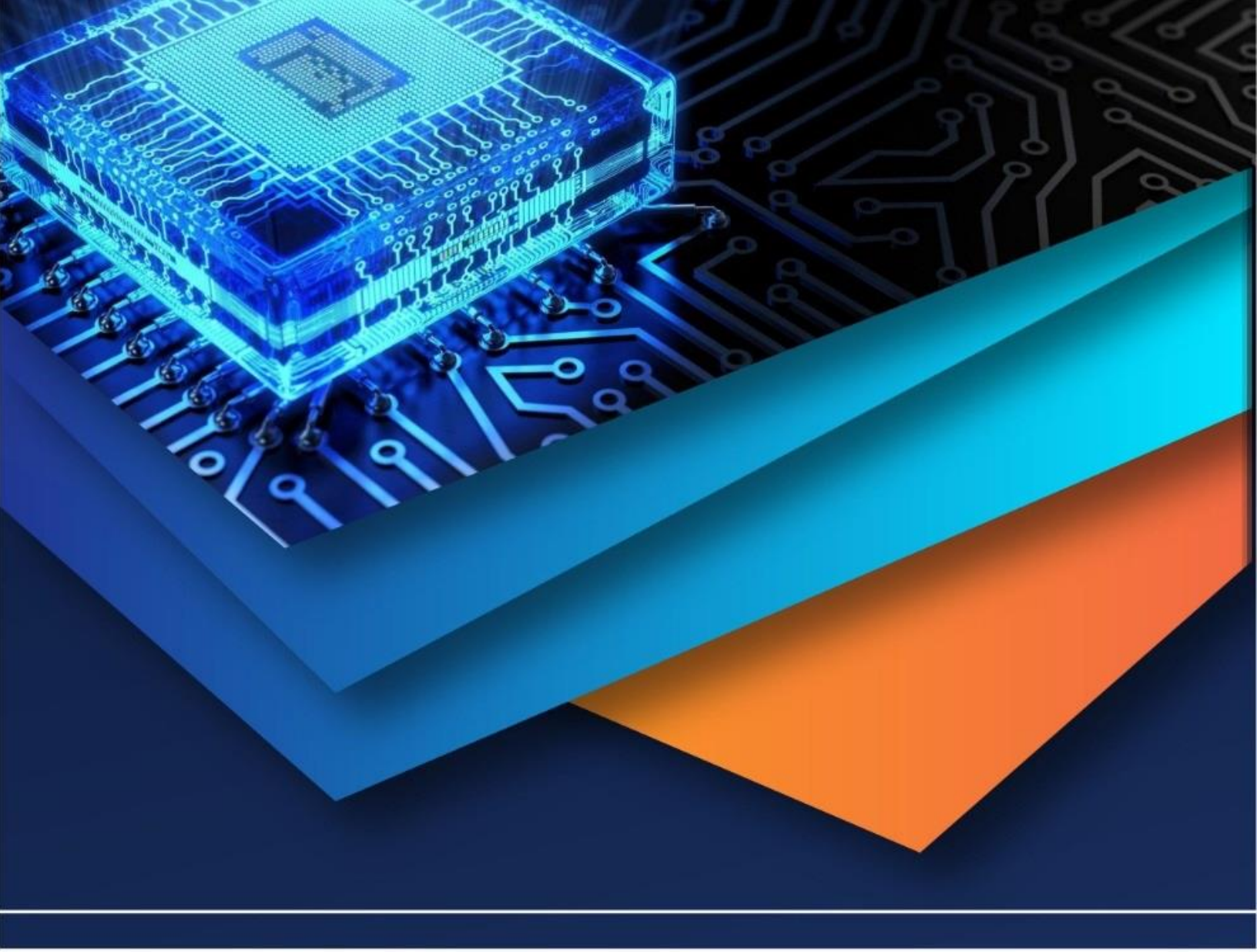
[6] Alwi N. H. M., Fan I. S.,"Threats analysis for elearning",*International Journal of Technology Enhanced Learning*, 2010,2(4),358-71.

[7] Apampa K. M., Wills G., Argles D. "An approach to presence verification in summative e-assessment security", International Conference on Information Society (i-Society 2010), 2010, IEEE.

[8] Shaver C. D., Acken J. "Effects of equipment variation on speaker recognition error rates", International Conference on Acoustics Speech and Signal Processing (ICASSP), 2009, IEEE.

[9] Ullah A., Xiao H., Lilley M. "Profile Based Student Authentication in Online Examination", International Conference on Information Society (i-Society 2012), 2012, IEEE.

Zhao Q., Ye M. "The application and implementation of face recognition in authentication system for distance education", 2nd International Conference on Networking and Digital Society (ICNDS), 2010, IEEE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY