International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206666

Graphical User Authentication Using Hybrid Visual Cryptographic Technique

S. Sivagama Sundari*[1], Dr. K. Kuppusamy[2]
*[1]Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu, India
[2]Department of Computational Logistics, Alagappa University, Karaikudi, Tamil Nadu, India

Article Info
Volume 6, Issue 6
Page Number: 350-355
Publication Issue :
November-December-2020
Article History
Accepted : 20 Dec 2020
Published : 30 Dec 2020

ABSTRACT

User authentication is the important aspect while offering common and utility services. Most of the web services are authenticates the exact user by using the traditional login model but it has security risks. Graphical user authentication is the replacement to solve the issues in traditional model. The research proposes a new graphical based user authentication model (VerCube) using a hybrid approach. This model implements the cryptographic technique and visual cryptographic representations.

Keywords : DES, TDES, Visual, Authentication, Graphical Password

I. INTRODUCTION

The World Wide Web has a huge list of websites which are offering variety of web based services called E-Services. These web services are ensures the data security through the user authentication approaches. User authentication is mandatory while offering a service to restrict unauthorized users. The traditional or mostly used approach is the login. The login inputs the username and password from the user. The password can be a combination of alphabets, numbers and special symbols. Most of the websites allow the user to create their own password and some other websites are generating automated random passwords [1].

At the time of login, the user has to provide the exact password and the password will be validated and verified by the websites. The authenticated user can be redirected into the next stage. The traditional login model is easy to implement but it has risks. The password can be hacked easily using random methods, keystroke tracking, OCR and unique identity guesses [5].

The graphical user authentication is the newest model which is suggested to offer high security than the usual login approach. The graphical authentication is the concept of using graphical objects such as shapes, pictures instead of alpha numeric values.

The Graphical authentication offers high security because of it does not let the attacker to steal the password in any other ways which are mentioned above. The graphical method can offer variety of advantages like attraction, easier remembrance, implementation support and high security than the traditional approach.

This research work suggests a hybrid model of graphical user authentication with a high secured way. This proposed work implements the TDES Cryptographic algorithm and Visual Cryptographic approaches to provide the graphical user authentication.

Visual cryptography is the way of transfer and retrieves secret data by using pair images. The data is hidden within the pair images and the receiver can get the data by overlaying the image pairs. This work uses the visual cryptography model to hide an encrypted secret code and the code can be retrieved by overlaying the images. The data encryption and decryption are done by the TDES algorithm. The proposed implementation algorithm is named as VerCube Graphical Authentication algorithm. The VerCube is a fully automated graphical authentication algorithm and it includes three automated stages.

II. RELATED WORKS

Paper titled "Accessing And Study of Cloud Services Using Graphical Password Authentication", authored by Jasmin P. Bhootwala and Pravin H. Bhathawala, Published in 2019. The authors proposed a new graphical password authentication scheme which is based on the alphabets. The model applies an alphabet sequence number to every letter in username. Similarly the model assigns a letter between A-I by the sum of the digits in the total of sequence number called SET. The model has 100 different images in every SET and user has to select two images from the 100 images at the time of login [2].

Paper titled "Secure User Authentication And Graphical Password Using Cued Click Points", authored by Saraswati B. Sahu and Angad Singh, Published in 2014. The authors suggested a graphical authentication model by based on the click points. The model lets the user to upload an image or video from the local system at the time of registration. The user can choose various click points on over the image or on over the video frame. At the time of login, the user has to click the same click points on the same image file [3].

Paper titled "Encrypted Negative Password Using RSA Algorithm", authored by Salva P.B and Nice Mathew, Published in 2019. The authors proposed a cryptographic based negative password scheme. The work encrypts the actual text password and a negative password will be created after the encryption. The negative password is also encrypted and it is called as Encrypted Negative Password. The model proposed a multilevel based encryption scheme to the textual password [4].

III.PROPOSED MODEL

The VerCube Model is a hierarchy based automated graphical user authentication scheme. The proposed model is a combination of Cryptographic approach and Visual Cryptography scheme. The model strongly suggests the traditional login authentication to be done before the graphical authentication to offer high security. After the successful login, the VerCube unit begins its functionality.

The VerCube scheme first generates a random secret code. The secret code will be encrypted into encrypted secret code by TDES algorithm. The model has an internal source of image data set. A pair of images will be selected from the image data set randomly by the image loader unit. The encrypted secret code will be divided into two portions and the every portion will be encoded in every image using LSB scheme without destroying the image quality. The resulting images are having the encrypted secret code in its pixels.

Fig 1 – Encryption and Encoding Flow

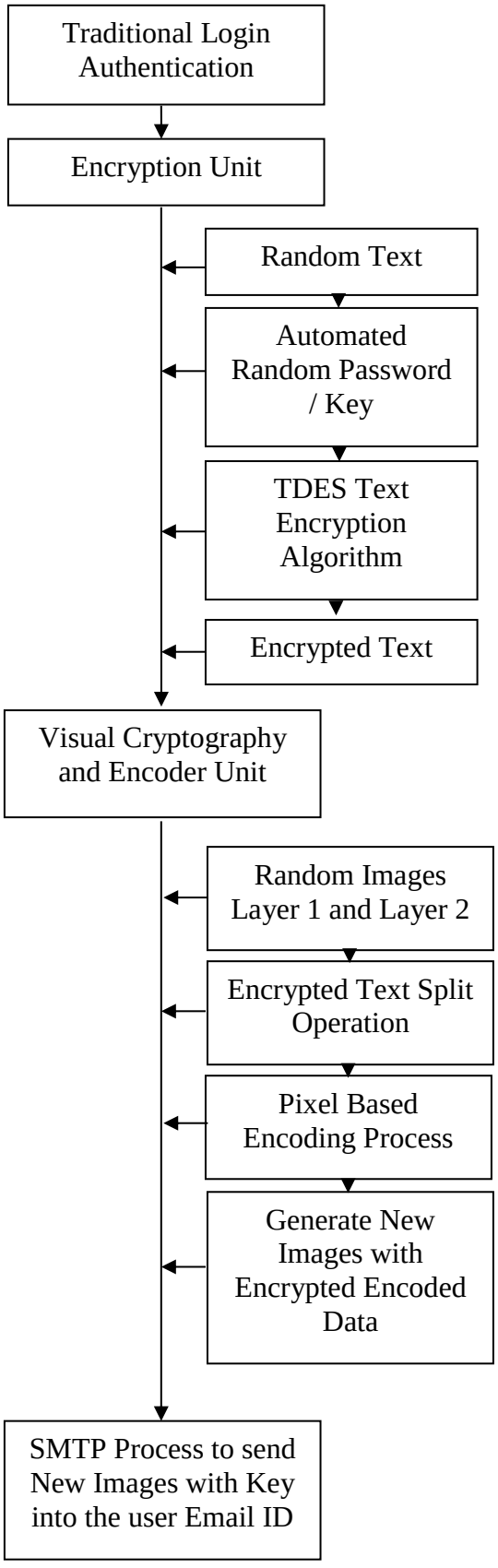
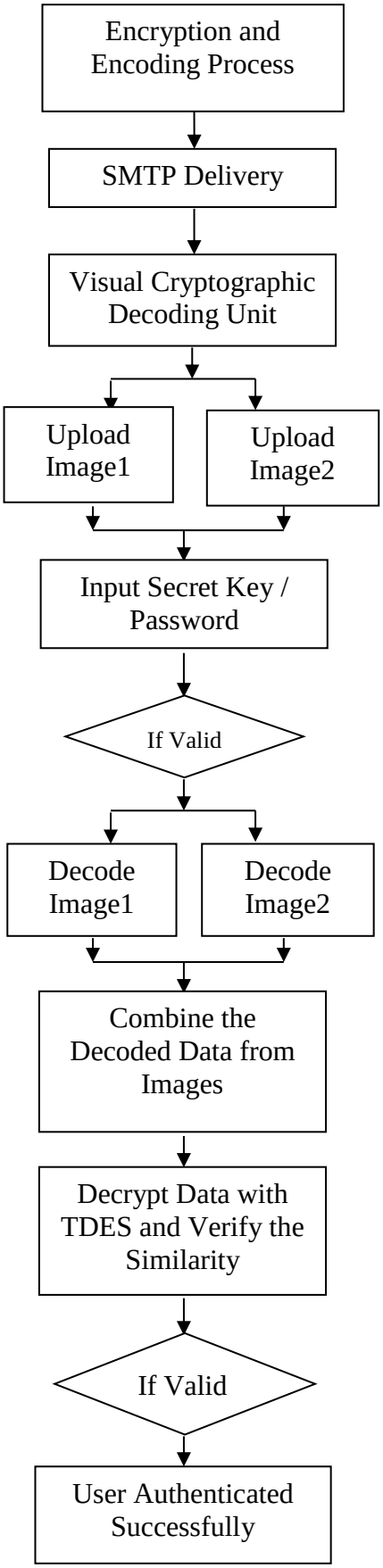


Fig 2 – Decoding and Decryption Flow



The encoded images and the encryption key can be transferred to the currently logged user's Email ID using SMTP functionality. The encryption stage, portion division stage, encoding stage and SMTP are fully automated and the model suggests the above stages should be performed after the traditional login verification. The user has to download the pair images and encryption key from the registered Email ID for graphical authentication. The Authentication Verifier unit is implemented to verify the exact user via the VerCube Model.

The current user has to upload the pair images in the sequence with the decryption key. The model loads the image pixels and verifies the data availability. The model begins to start the decoding process after the verification. The LSB scheme is applied to retrieve the encrypted secret code from the pixels in both image pairs. The retrieved secret code will be decrypted by the user's decryption key. The actual secret code will be verified from images pairs and successfully authenticates the user if the verification becomes successful.

IV.PROPOSED ALGORITHM

The VerCube is the proposed algorithm in the research work. The VerCube is a graphical user authentication model which can verifies an user using three internal stages. The stages are categorized as encryption stage, portion division stage and encoding stage.

VerCube Encryption Algorithm:

Step 1: Begin

Step 2: User Authentication using the Traditional Login

Step 3: Random Secret Code Generation

Step 4: Random Encryption and Decryption Key Generation

Step 5: Random Image Pair Selection

Step 6: Encrypt the Secret Code with Key using TDES Algorithm

Step 7: Divide the Encrypted Secret Code into Two Portions

Step 8: Load Images Pixels in Every Image

Step 9: Encode First Portion in Image1

Step 10: Encode Second Portion in Image2

Step 11: Create New Image Files

Step 12: Transfer the New Images Files into the User Email ID using SMTP with Key

Step 13: End

The above steps are fully automated without any manual interaction. The user authentication takes place after the completion of above algorithm.

VerCube User Authentication and Decryption Algorithm:

Step 1: Begin

Step 2: Image1 Loader and Verifier Unit

Step 3: Image2 Loader and verifier Unit

Step 4: Encrypted Secret Code Availability Check

Step 5: Data Decoding Process from Image1 and Image2

Step 6: Decryption Key verification

Step 7: Data Merge Process and retrieve the actual Encrypted Secret data

Step 8: Data Decryption by TDES decryption algorithm.

Step 9: Verification of Actual data and Decrypted data

Step 10: If similar, then authentication success otherwise authentication failed.

Step 11: End

The user authentication and decryption algorithm has the following stages like the encryption algorithm called Pixels loader stage, Encrypted secret code retrieval stage, decryption stage and authentication stage.

V. EXPERIMENTAL RESULT

The VerCube graphical authentication algorithm's process flow is implemented with GUI environment and the result stages are explained below:

Fig – Traditional Login

The Traditional login is the initial stage and the graphical authentication unit will be redirected once the user passes this login stage.

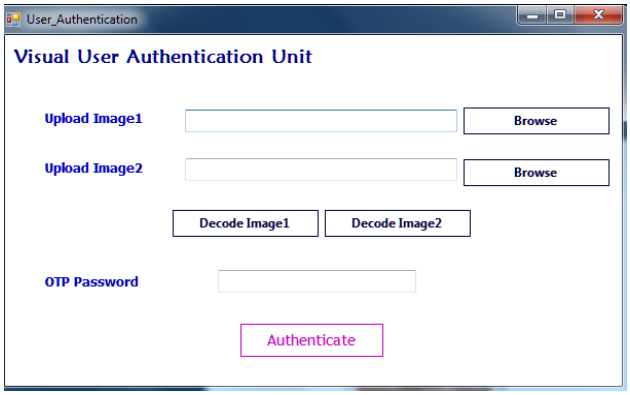


Fig – User Authentication Unit

The VerCube encryption algorithm is a fully automated random scheme and it starts processing after the completion of login stage. It is a hidden model and processes in background. The encryption algorithm sends two image files with a decryption key into the user's email Id. The images files are having the encrypted secret code in its pixels which is encrypted with TDES. The user has to download the files and upload into the User Authentication Unit. The unit verifies the image data availability and starts data decoding process. The retrieved data will be decrypted with the decryption called OTP password. The unit verifies the secret code from the two images and performs a similarity comparison with actual code. Generates the authentication result by based on the comparison result.

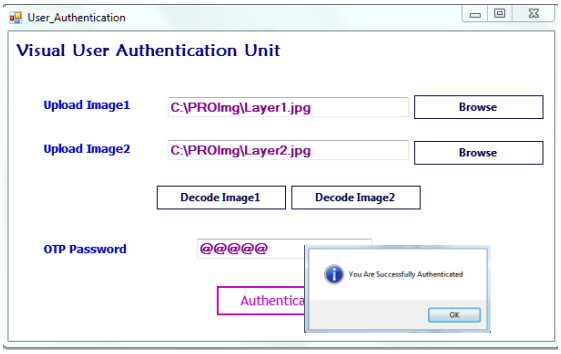


Fig – Successful Authentication Alert

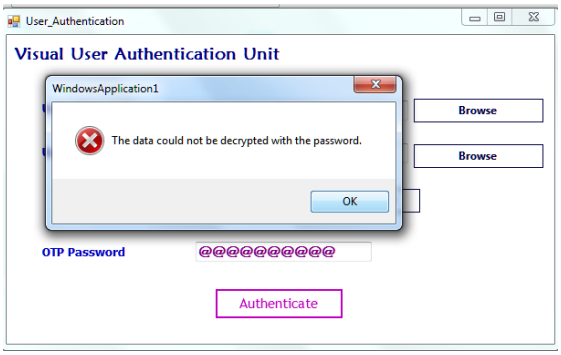


Fig – Authentication Failed Alert

VI. CONCLUSION

The VerCube algorithm based model is a three layered authentication scheme and it can be implemented for any platform like cloud servers, mobile apps and third party services. This model includes TDES cryptographic algorithm because of the security needs and faster performance. The model

consumes low processing time than the existing models and offer high security than others.

VII. REFERENCES

[1]. Aakansha Gokhale and Vijaya Waghmare, “Graphical Password Authentication Techniques: A review”, International Journal of Science and research, ISSN: 2319 - 7064.

[2]. Jasmine P. Bhootwala and Dr. Pravin H. Bhathawala, “Accessing and Study of Cloud Services Using Graphical Password Authentication” International Journal of Engineering And Technology, ISSN: 2278 - 0181.

[3]. Miss. Saraswati B. Sahu and Angad Singh, “Secure User Authentication And Graphical Password using Cued Click Points” International Journal of Computer Trends and Technology, ISSN: 2231 - 5381.

[4]. Salwa P.B and Nice Mathew, “Encrypted Negative Password Using RSA Algorithm”, International Research Journal of Engineering and technology, ISSN: 2395 - 0056.

[5]. Reshma and G. Shivaprasad, “Research and Development of User Authentication using Graphical Passwords: A prospective methodology”, International journal of Innovative Technology and Exploring Engineering, ISSN: 2278 - 3075.

Cite this article as :

S. Sivagama Sundari, Dr. K. Kuppusamy, "Graphical User Authentication Using Hybrid Visual Cryptographic Technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 6, pp. 350-355, November-December 2020. Available at doi : https://doi.org/10.32628/CSEIT206666

Journal URL : http://ijsrcseit.com/CSEIT206666