IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Visual Cryptography and OTP Against Phishing Threats

[1]Angelin Rosy M, [2]Anusha M

[1,2]Department of Master of Computer Applications,
[1,2] Er. Perumal Manimekalai College of Engineering,
Hosur,

Abstract : The web-based application named "Visual Cryptography and OTP Against Phishing Threats" implements Microsoft ASP.NET 2022 as front-end technology while Microsoft SQL Server 2019 functions as its backend management system. The majority of digital platforms currently use user authentication approaches through combination of usernames and passwords. The phishing threat remains a fundamental security issue since attackers manipulate users through deception to obtain password details and monetary information causing identity theft and financial fraud. The integration of Visual Cryptography with OTP-based verification creates a strong protective system which successfully decreases phishing vulnerability. Attackers cannot obtain access permissions to both shares nor predict CAPTCHA contents which results in substantial reduction of unauthorized entry attempts.

IndexTerms - Authentication Security, One Time Password, Visual Cryptography.

INTRODUCTION

Cyber threats are becoming more dominant because phishing attacks use fake legitimate platform presentations to steal confidential data including passwords and banking information and personal identifiers from users. The schemes use fabricated websites together with deceptive emails which mimic trusted platforms. The growing issue demands significant implementation of multi-layered defensive measures.

This project introduces a novel method that merges Visual Cryptography with One-Time Passwords (OTP) to strengthen authentication and reduce phishing vulnerabilities. Visual Cryptography works by splitting an image into several transparent layers, or shares, which individually reveal nothing. Only when these shares are accurately combined does the original image become visible, adding a secure layer that is extremely difficult to counterfeit or reconstruct without authorized access. Complementing this, OTPs offer dynamic, session-specific codes that change with each login, ensuring that reused or intercepted credentials have no value to attackers.
The integration of these two technologies offers a dual defense system: even if a user interacts with a fraudulent site, the attacker cannot access the complete visual key or generate a valid OTP. This significantly lowers the success rate of phishing scams.

Through their work Dhamija et al. [1] studied how phishing victims get deceived. The authors stressed the requirement to develop better authentication techniques which could successfully combat these security vulnerabilities.

The research conducted by Ateniese et al. [2] introduced general access structures into visual cryptography to allow multiple parties to exchange secure information through permission-controlled definitions.

Alsharnouby et al. [3] evaluated how users deal with phishing threats using their research about security systems that unify visual warnings with multiple authentication steps.

Researchers studied multiple visual cryptography techniques extensively according to Chandramathi et al. [4] because they wanted to determine their value in digital image authentication and distribution security.

Secure graphical passwords utilizing visual cryptographic techniques were created by Pillai et al.[5] for phishing protection.

The authors of Choudhury et al. [6] built an OTP authentication method which uses visual cryptography to enhance financial security by guarding users from phishing threats.

PROPOSED WORK

1. High Security Constraints are used here to protect the users from Phishing Websites
2. Random One Time Password (OTP) has been fixed as security feature for Email Validation as well as for Payment Gateway form.
3. Image Captcha models are used for Share dividend process.
4. User and Adminstrator side share dividend with OTP based file key names fixed in the share file.
5. Case Sensitive Share file names are designed.
6. Users are highly protected with Visual Cryptography and One Time Password combination.

METHODS

User Registration

The user presents individual key information including username, password and email through the user registration process. Users must supply an image choice through an interface where they get a dual 2-out-of-2 visual cryptography process to generate two separate images. Through this approach the image gets divided between two distinct visual shares. Two parts of the image are generated by the system where the first part remains on the server and the second part is given to the user. Single shares by themselves do not provide meaningful information yet the combination of them will provide the user with access to the original image. The method creates a secure identity confirmation system while at the same time providing stronger protection against phishing distractors.

One Time Password Generation

One-Time Password (OTP) presents a short-lived security code that functions as a single-time authorization element for accessing an account or conducting a verification process. OTPs operate differently from traditional passwords since they exist only for one-time use and expire quickly after generation or when used even if they worked before. The limited usage period of OTPs turns them into effective tools for blocking replay attacks. These security keys serve as an essential component of 2FA systems since users need to authenticate with both their memorized passcode and the time-sensitive token that they receive through a secure channel.

User-Email Validation

The verification process checks that submitted email addresses belong to an existing and reachable user while proving actual ownership. The feature plays an essential part in authentication processes to protect against unauthorized access of fake accounts in registries.

Step-by-Step Process:

1.User Submits Email: The user provides their email address at the moment of account creation through sign-up.

2. System Creates a Verification Key: The system generates a special link or code that belongs to a single user only.

3.Verification Email is Sent: The system automatically sends this link through email to the recipient's inbox.

4. User Clicks the Link: Clicking the verification URL present in the email prompts the user to send a server request to the application.

5. Validation Check: The server matches the verified token which came through against its current records. The system verifies the user when the entered token matches an active token.

6. Full Access Enabled: Users gain total system access through verified functionalities once their email address has been validated properly.

Share Dividends

Email-based authentication becomes stronger when cryptographic methods including visual encryption (shown in fig 2) and threshold-based secret splitting are used. The system creates separate parts from the secret code to act as verification shares instead of sending a complete verification code. A share validation occurs after the system combines its separated shares properly.

The sharing distribution technique provides confidentiality by making individual code elements nonsensical since they cannot reveal significant authentication data on their own. Consequently this approach makes it difficult for unauthorized parties to gain access via intercepted messages or brute force attacks. This figure 1 illustrates how visual cryptography with one time passwords fights against phishing threats.

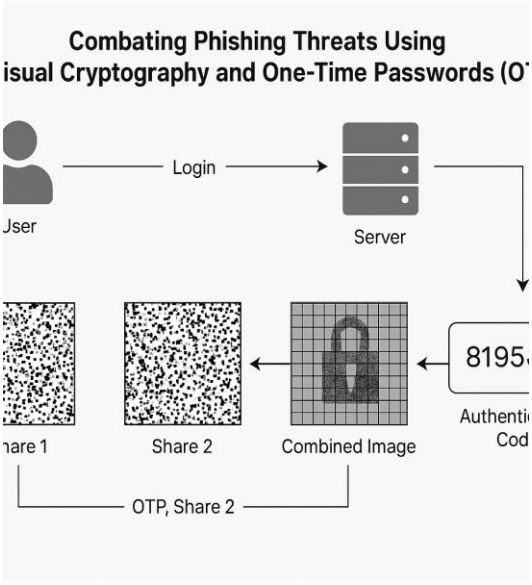


Figure 1: System architecture

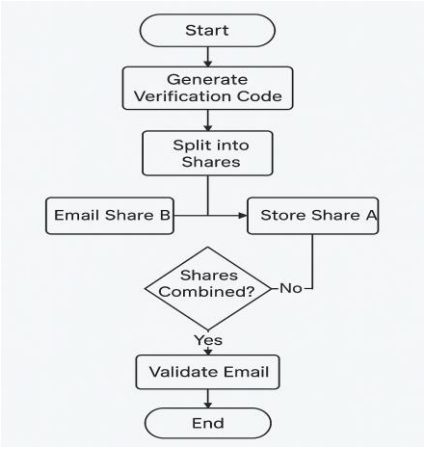


Figure 2: Divid architecture

User Login

Before granting digital platform access user login functions through identity verification to authenticate personnels. Users need to input their personal details such as email or username before providing an access key such as password which is displayed in fig 2.

Generate Share

Emergency modifications to shares can be accomplished through the link which generates a share menu for users. The share generation form follows a procedure that matches exactly like the email validation and dividend sharing procedure.

Payment Form

When moving to the payment form users must validate their email address through a One-Time Password (OTP) protocol. At this point the user can upload their share contents to be integrated with the server's share. Users must successfully compare the combined entered value against the database record which activates an image captcha field for an additional verification step where the user-operator must type the same string as displayed. After successful captcha validation the user will receive access to the payment finalization page.

Administrator-Image Master

Captcha image lifecycle management becomes the key task for an Administrator Image Master in the verification process. The administrator of the image master team supports image management by establishing image storage and display procedures and securing both the image database and the image verification system for maximum reliability. The administrator applies captcha images according to correct procedures to preserve system performance which blocks automatic activities and prevents unapproved actions.

Administrator-View Payment History

Authorized administrators receive full transaction details through payment history logs which they can view. Through this system administrators track payment status while performing parameter-based searches to detect questionable payment activities. The administrator gains full visibility of chosen financial transaction data points which include amounts and dates and payment methods together with user-linked data while ensuring accurate financial records.

Preprocessing

The use of preprocessing techniques with visual cryptography and OTP systems increases phishing threat protection across both systems. The data cleaning procedures follow a thorough pace and authentication systems ensure security against phishing risks while these operations take place.

RESULTS

The system operates effectively to detect phishing attacks immediately and creates secure visual authentication procedures for users during approval processes. The system creates a reliable platform for future security integration by enabling biometric or blockchain technologies since both are depicted in Figs.

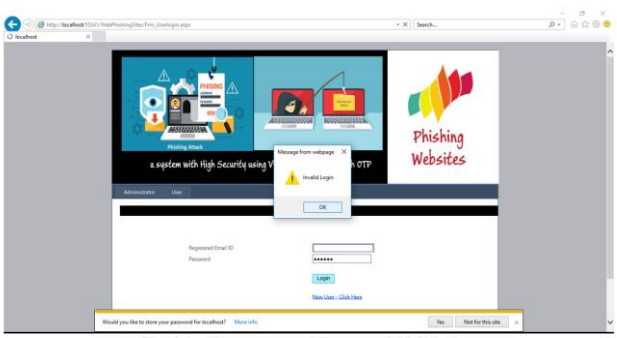
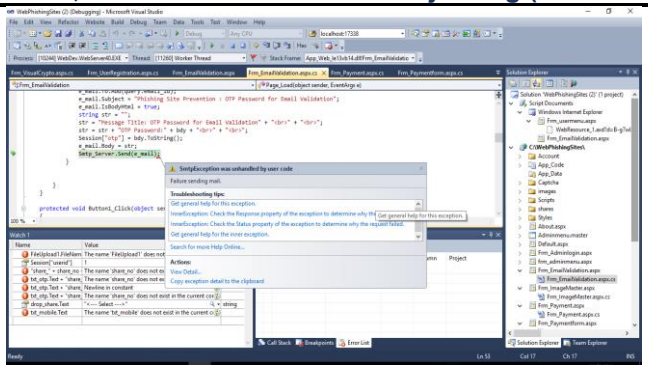
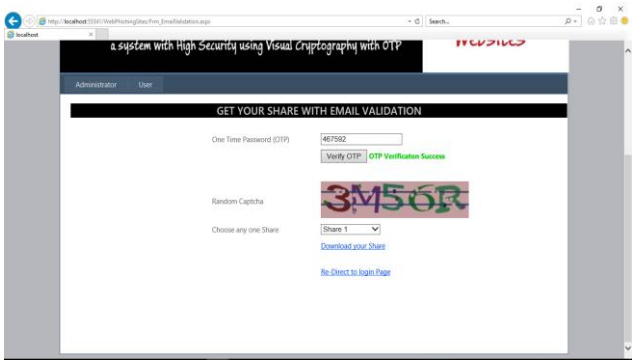


Fig 4.1 : Username and Password Validation





CONCLUSION

This project establishes an advanced method to combat phishing threats by using Visual Cryptography with One-Time Password (OTP) technology. The system protects data authenticity and user identification through secure OTP development together with image improvement steps coupled with dual verification procedures.

The system uses visual cryptography mechanics that split user-based images into shares alongside time-sensitive OTPs to minimize unauthorized access attempts. The preprocessing procedures simultaneously boost system accuracy while protecting against conventional phishing attempts which makes the model appropriate for real-world deployment while ensuring security.

The developed authentication framework offers a resilient solution against phishing threats while appropriately addressing end-user needs for easy operation.

Conflict of Interest: The authors have verified that this study lacks any conflicting interests.

Funding Disclosure: There was no financial support or third-party funding used for performing this research project.

Ethical Approval: The researchers performed this study devoid of experiments which included human or animal participants.

Consent Disclosure: The study omitted patient-related data so consent procedures were not required.

ACKNOWLEDGMENT

The authors declare that they have no reports of acknowledgments for this

REFERENCES

[1] Tariq Mian M. and Khan Kamran M. developed an advanced anti-phishing system that combined visual cryptography with RSA encryption for secure communications in the International Journal of Computer Science and Network Security volume 17 issue 2 pages 27–33 during 2017.

[2] Rao, P. Venkata Subba and T. Sridevi provided an anti-phishing technique using visual cryptography in "An anti-phishing technique based on visual cryptography" which appeared in International Journal of Network Security & Its Applications volume 3 issue 4 pages 181–192 in 2011.

[3] The authors present image sharing methods through visual cryptography using authentication mechanisms in "Pattern Recognition Letters" issue 27 volume 6 starting on page 597 in 2006.

[4] The database approval method discussed by Chadwick David W. at the IFIP International Conference on Communications and Multimedia Security earned recognition during 2003 through page 311–326.

[5] Lin Chih-Cheng together with Wen-Hsiang Tsai published "Secret image sharing with steganography and authentication" in Journal of Systems and Software vol. 73 no. 3 pp. 405–414 during 2004.

[6] Wu and Tai's "An efficient visual secret sharing scheme using quadratic residues" appeared in Mathematics and Computers in Simulation during 2004 with volume number 64 and first issue page range 95-107.

[7] Goriparthi alongside Kota Reddy and M. Padmavathamma introduced an anti-phishing framework through visual cryptography in International Journal of Computer Applications vol. 55 no. 7 (pp. 31–35, 2012).