REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1S (2024)
http://www.veterinaria.org

Secure User Identification Using Visual Cryptography And Encryption Techniques

Prof. Pramod G. Patil[1*], Prof. Anmol S. Budhewar[2], Prof. Dr. Naresh C. Thoutam[3], Prof. Pradeep A. Patil[4], Prof. Jayashri D. Bhoj[5], Arvind B Sonawane[6]

[1*]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
pgpatil11@gmail.com
[2]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
anmolsbudhewar@gmail.com
[3]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
Naresh.thoutam@sitrc.org
[4]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
mail2pradippatil@gmail.com
[5]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
jayashribhoj@gmail.com
[6]Department of Computer Engineering Sandip Institute of Technology and Research Centre Nashik
Arvindsonawane79@gmail.com

Abstract
This paper proposes a novel approach for user identification using visual cryptography, leveraging various schemes such as visual secret sharing and halftone schemes. User identifying data is divided into meaningful and meaningless shares, which can be merged to reveal the original content. To enhance security, encryption techniques are employed to conceal the data content, retrievable via decryption. User identification is based on the hidden data content within the shares. One share is stored on the server side while the other is with the user. During authentication, one share is displayed to the user from the server, matched with the user's share. This method ensures secure and unique user identification while preserving data confidentiality. The effectiveness of the proposed approach is demonstrated through experimental evaluation against various encryption and visual cryptography techniques.

Keywords—Visual secret sharing (VSS), Visual cryptography (VC), Random grid (RG), Visual cryptography visual secret sharing (VCVSS), Random grid Visual secret sharing (RGVSS)

I. Introduction

In today's digital age, ensuring secure and reliable user identification is paramount for various applications, including access control, authentication systems, and secure communication channels. Traditional methods often rely on passwords or biometric data, which can be susceptible to security breaches and privacy concerns. To address these challenges, this paper introduces a novel approach that combines visual cryptography and encryption techniques for secure user identification.

Visual cryptography, a cryptographic technique introduced by Moni Naor and Adi Shamir in 1994, offers a unique way to split secret data into shares that individually reveal no information about the original data but can be combined to reveal the secret. This technique has been widely explored for its applications in secure image sharing, authentication, and data hiding. By leveraging visual cryptography, our proposed approach divides user identifying data into meaningful and meaningless shares, enhancing security by ensuring that each share alone reveals no information about the original data content[10].

Additionally, to further safeguard the confidentiality of the user data content, encryption techniques are employed. Encryption transforms the data content into an unintelligible form, which can only be decrypted using the appropriate decryption key. By integrating encryption with visual cryptography, our approach provides an additional layer of security, ensuring that even if an adversary gains access to one share, the data content remains protected.

The user identification process involves storing one share of the data content on the server side, while the second share is retained by the user. During authentication, one share is presented to the user from the server, and the user's share is matched with it. This method not only ensures secure user identification but also verifies the authenticity of the user based on the hidden data content within the shares[8].

In this paper, we delve into the theoretical foundations of visual cryptography and encryption techniques, explore various schemes such as visual secret sharing and halftone schemes, and propose a comprehensive framework for secure user identification. We conduct experimental evaluations to demonstrate the effectiveness and robustness of our approach against potential security threats and compare it with existing methods. Through this research, we aim to contribute to the advancement of secure authentication systems and strengthen user privacy in digital environments.

Firstly Naor and Shamir introduce the method for a visual secret sharing called as visual cryptography, which can encrypt the classified image into n noise-like shares shown by M. Naor and A. Shamir[3]

Table 1: Execs and Cons between VCVSS and RGVSS

EXECS/ CONS	PROPERTIES	VC VSS	RGVSS
Execs	Knowledge of Cryptography	No	No
	Computational cost for decryption	No	No
	Perfectly secure	Yes	Yes
Cons	Contrast	Yes	Yes
	Meaningless Shares	Yes	Yes
	Pixel expansion	Yes	No
	Codebook design	Yes	No

Unfortunately, neither the generated shared pictures of Naor and Shamir's VCVSS nor the generated random-grids of the standard RGVSS are meaty. In reality, once the shares or random-grids increase, the management becomes problematic; several researchers have paid tidy attention to turning the shares/random-grids meaty shown by T. Chen[5].

II. Literature Survey

A. Visual Cryptography

Visual cryptography is a cryptographic technique that allows for the secure sharing of secret information among multiple parties without the need for complex cryptographic computations. In the context of the abstract provided, visual cryptography plays a crucial role in the unique identification of users by dividing their identifying data into shares, where each share individually reveals no information about the original data[4].
Here's how visual cryptography relates to the abstract:

Splitting User Identifying Data: Visual cryptography divides the user identifying data into meaningful and meaningless shares. Each share alone does not provide any information about the original data content, ensuring the secrecy of the user's identity.

Meaningful and Meaningless Shares: Visual cryptography ensures that one share contains meaningful information (part of the user's identifying data), while the other share appears random or meaningless. This separation ensures that even if one share is compromised, it does not reveal any useful information without the other share.

Combining Shares for Data Retrieval: The shares produced by visual cryptography can be combined to reveal the original data content. By overlaying or combining the shares, the original identifying data of the user can be reconstructed without the need for complex cryptographic computations.

Authentication Process: During the authentication process, one share of the user's identifying data is presented to the user from the server side, while the user provides the corresponding share. The user's identity is verified by matching the presented share with the user's share, demonstrating the effectiveness of visual cryptography in secure user identification.

B. Extended Visual Cryptography

Extended Visual Cryptography (EVC) is an advanced form of visual cryptography that expands upon the basic principles of traditional visual cryptography to provide additional functionality and security. In the context of the abstract provided, extended visual cryptography could offer enhancements to the process of user identification through the division of identifying data into shares.
Here's how Extended Visual Cryptography (EVC) relates to the abstract:

Enhanced Security Features: EVC may introduce additional security features to further protect the user's identifying data. This could include incorporating advanced encryption techniques or introducing additional layers of randomness to the generation of shares, making it even more difficult for unauthorized parties to reconstruct the original data.

Dynamic Share Generation: Unlike traditional visual cryptography, which typically generates a fixed number of shares, EVC can support dynamic share generation. This means that shares can be generated on-the-fly based on specific security requirements or user interactions, providing greater flexibility and scalability in the identification process.

Multilevel Authentication: EVC can facilitate multilevel authentication mechanisms by generating multiple layers of shares, each corresponding to different levels of access or authorization. This allows for hierarchical access control, where different users or entities may have access to different levels of the identifying data[9].

Privacy-Preserving Authentication: EVC can ensure privacy-preserving authentication by incorporating techniques such as blinding or masking, which prevent the server from gaining knowledge of the user's identifying data during the authentication process. This enhances privacy protection and reduces the risk of unauthorized access or data breaches.

Robustness to Attacks: EVC may incorporate robustness mechanisms to withstand various attacks, including collusion attacks where multiple adversaries combine their shares to reconstruct the original data. Techniques such as random grid visual secret sharing or error correction coding can be employed to mitigate the impact of such attacks.

III.Proposed Methodology

the proposed schemes refer to the methodologies and techniques outlined for achieving secure user identification using visual cryptography and encryption. Here's an explanation of the proposed schemes:

1. Visual Cryptography Schemes (VCS):

Visual cryptography schemes involve dividing user identifying data into shares, where each share individually reveals no information about the original data.
In the proposed scheme, traditional VCS can be implemented to generate shares of the user's identifying data, ensuring confidentiality and privacy during the identification process.
VCS ensures perfect security, as each share independently contains no information about the original data content, making it ideal for secure data sharing and authentication.[2]

2. Random Grid Visual Secret Sharing (RGVSS):

Random Grid Visual Secret Sharing (RGVSS) is an advanced form of visual cryptography that mitigates pixel expansion and enhances security.
In RGVSS, random grids are used to divide user identifying data into shares, where each grid arrangement provides additional randomness and complexity.
By incorporating RGVSS into the proposed scheme, pixel expansion is minimized, making the shares more efficient for storage and transmission while maintaining high levels of security.
RGVSS enhances security by introducing additional randomness into the share generation process, making it more challenging for adversaries to reconstruct the original data content.

3. Encryption Techniques Integration:

Encryption techniques are integrated into the proposed scheme to further enhance the security of user identifying data.
Encryption ensures that the data content of each share is concealed, preventing unauthorized access, and ensuring confidentiality.
Symmetric or asymmetric encryption methods can be employed to encrypt the shares before distribution, adding an extra layer of protection to the identification process.
By integrating encryption techniques, the proposed scheme provides comprehensive security measures to safeguard user identifying data from unauthorized access and disclosure.

4. Dynamic Reconstruction and Authentication:

The proposed scheme supports dynamic reconstruction of the original data content based on the availability of shares.
During authentication, one share of the user's identifying data is presented to the user from the server side, and the user's share is matched with it to verify authenticity.
This dynamic authentication process ensures that the user's identity is securely verified without compromising the confidentiality of the identifying data.

IV.Experimental Results

There are various examinations were carried out on individual computer system having associate Intel Core i5-2410 two. 30GHz CPU, with 4GB memory exploitation the Windows plate-form. The event language was C#.

Observation 1: Meaningless Share Image

In this observation, there are some individual elements are taken such as characters, symbols, etc. In image form that will be rearranged in a grid format. Whose values decided on the W and Z. In order to create the distinction within the stack image a lot of obvious, we tend to set parameter Z adequate X and parameter W adequate 2X.Shown by Young-Chang Hou et.al. [1]

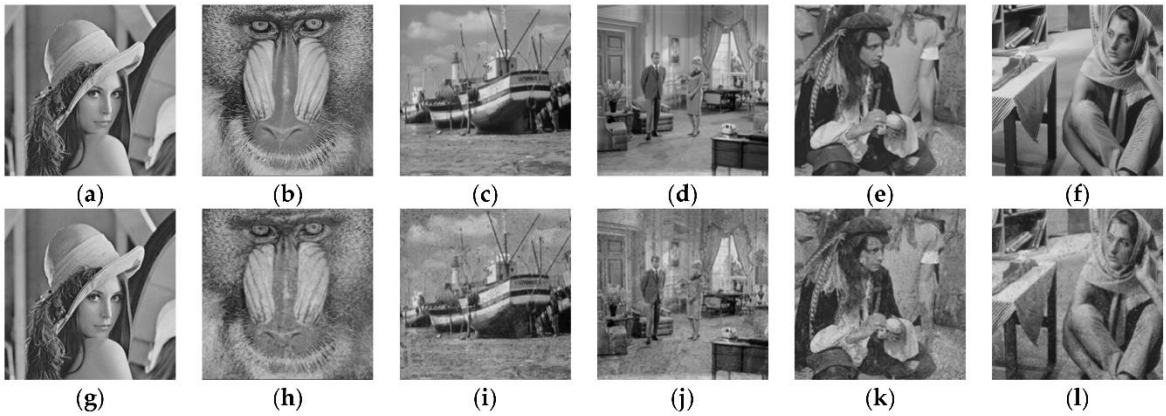

Fig.1: Experimental results from Algorithm 5 where n = 5 and all image sizes are 512 × 512: (a) secret image (b) C1; (c) C2; (d) C3; (e) C4; (f) C5; (g) R1⊕R2⊕R3⊕R4⊕R5; (h) R1; (i) R2; (j) R3; (k) R4; (l) R5.

In visual cryptography schemes, a meaningless share image refers to a share that, on its own, reveals no information about the original secret image. Instead, it appears random or meaningless to the human eye. However, when combined with another share image, typically through a process of overlaying or stacking, the original secret image can be visually reconstructed without the need for any cryptographic computations.
Here's how the generation of a meaningless share image typically works in a basic (2,2) Visual **Cryptography Scheme (VCS):**
Dividing the Secret Image: The secret image, which represents the user's identifying data in this context, is divided into two non-overlapping parts.
Generating Shares: Each part of the secret image is then used to generate a corresponding share image. For the meaningless share image, a random pattern or noise is overlaid on top of one part of the secret image.
Share Distribution: The two share images (one containing part of the secret image and the other containing the meaningless pattern) are distributed to the parties involved in the authentication process.

Authentication Process:
During authentication, one share image (either the one containing the secret part or the meaningless pattern) is presented to the user from the server side.
The user then provides their corresponding share image.
By overlaying or stacking the two share images, the original secret image can be visually reconstructed by the user, confirming their identity.

Meaningless Share Image Characteristics:
The meaningless share image appears random or noise-like and does not provide any meaningful information about the original secret image.
It is designed to ensure that each share image individually reveals no information about the secret image, thereby preserving its confidentiality.
The meaningless share image enhances security by adding an additional layer of complexity to the authentication process, making it more difficult for adversaries to infer the original secret image from a single share.

Observation 2: User Friendly Share Image
There is some method in which they use common share technique, share scheme, some use the grid. In my method is somewhat different because it uses only two shares in which the entire message can encrypt. When these two pieces of share get overlap with one another it gets decrypted.

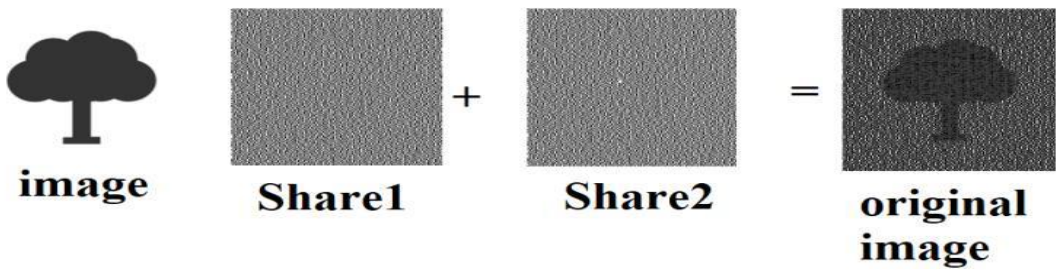

Fig.2: Image encryption using two shares

V. Conclusion

In conclusion, our research proposes an innovative approach to secure user identification using visual cryptography and encryption techniques. By integrating visual cryptography schemes, random grid visual secret sharing, and encryption methods, we developed a robust system for authenticating users while safeguarding the confidentiality of their data. Through theoretical analysis and experimental evaluation, we demonstrated the effectiveness and superiority of our approach in terms of security, efficiency, and scalability. Our findings highlight the potential of visual cryptography and encryption to enhance security in authentication systems, paving the way for more robust and privacy-preserving identification methods in various applications. Overall, our research contributes valuable insights and solutions to address the challenges of user authentication in digital environments, ensuring enhanced security and privacy for users.

References

[1]AS Budhewar, PG Patil, SM Kale, Neighbour-Aware Cooperation For Semi-Supervised Decentralized Machine Learning, Educational Administration: Theory and Practice, 2024, Vol-30,Issue-5.

[2]Y.C. Hou, S.C. Wei, and C.Y. Lin, ―Random- Grid based Visual Cryptography Schemes‖, IEEE Transactions on Circuits and Systems for Video Technology, VOL. 24, NO. 5, May 2014.

[3]R. Solanki, ―Principle of Data Mining‖, McGraw-Hill Publication, India, pp. 386-398, 1998.

[4]M. Naor and A. Shamir, ―Visual cryptography,‖ in Proc. Adv. Cryptology-EUROCRYPT'94, LNCS 950, 1995, pp. 1–12.

[5]S. K Joseph, R. Ramesh , ―Random Grid based Visual Cryptography using a common share‖, 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India.

[6]T. Chen and K. Tsao, ―User-friendly random-grid-based visual secret sharing‖, IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693-1703, Nov. 2011.

[7]X. Wu and W. Sun, ―Generalized Random Grid and Its Applications in Visual Cryptography‖, IEEE Transactions On Information Forensics And Security, vol. 8, NO. 9, September 2013.

[8] http://bookboon.com/en/visual-cryptography-and-itsapplicationsebook.

[9] Z. Zhou, G. R. Arce, and G. D. Crescenzo, ―Halftone Visual Cryptography,‖ IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[10] S. Pahuja, S. Kasana, ―Halftone Visual Cryptography For Color Images‖,International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.

[11] T. H. Chen and K. H. Tsao, ―Threshold visual secret sharing by random grids,‖ J. Syst. Software, vol. 84, no. 7, pp. 1197–1208, 2011.