Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 6
ISET 2024

Advancements and Applications of Anti-Fraud Graphical Passwords

Jiawen Shi

School of Computer Science and Engineering, Tianjin University of Technology, Tianjin, China

1811030504@stu.hrbust.edu.cn

Abstract. Visual cryptography represents a sophisticated and innovative approach to secure information sharing, gaining traction within the field of information security. This technology adeptly transforms sensitive data into visually interpretable graphics or images. These images are then segmented into multiple independent parts, each distributed among different stakeholders. This strategy ensures that no single party can access the complete data without collaboration, thereby enhancing security. This dissertation delves into several anti-fraud visual password schemes designed to mitigate risks associated with deceptive behaviors by participants and distributors alike. By addressing these vulnerabilities, the proposed schemes enhance the integrity and reliability of the data sharing process. The application of visual passwords in real-life scenarios not only bolsters data security but also shields private information from potential leaks. By reducing the complexity and cost associated with traditional decryption methods, visual cryptography offers substantial support for a wide array of application scenarios. This dissertation presents a comprehensive exploration of visual cryptography's potential to revolutionize data protection strategies, illustrating its importance and utility in contemporary digital environments.

Keywords: Visual Cryptography; Deceiver; Cumulative Matrix.

1. Introduction

With the rapid advancement of information technology, privacy protection and data security have become major societal concerns. Traditional cryptographic methods offer a certain degree of data security but are increasingly seen as complex, costly, and vulnerable to sophisticated attacks. Visual cryptography emerges as a novel branch within the field, simplifying the process of password creation, dissemination, and verification by using images. This approach not only makes password use more accessible to the general public, enhancing user competence, but also bolsters password security.

The concept of visual cryptography was first introduced by Naor and Shamir in 1994, presenting a secret-sharing scheme that divides a secret image into multiple sub-images. These can be recombined to reconstruct the original image, thereby enhancing the cipher's security by complicating the guessing process and increasing the cipher's variability, which in turn raises the difficulty of deciphering. The design also incorporates anti-spoofing measures, such as additional authentication mechanisms, to ensure the authenticity and validity of the shared images.

Current research in visual cryptography is showing promising developments. An increasing number of scholars and research institutions are focusing on this domain, achieving significant breakthroughs. As technology evolves and the scope of application expands, visual passwords have vast potential in various fields. In the context of the burgeoning Internet and digital era, the need for secure password mechanisms is becoming increasingly critical to safeguard personal privacy and data security. The research and application of visual cryptography hold significant value as an innovative method for enhancing password protection.

2. Anti-Fraud Visual Password Solution

Naor and Shamir have proposed the (k, n) threshold plan, the core idea of which refers to splitting a secret message into n parts and setting a threshold value k such that the original secret message can be recovered only if at least k parts are correctly combined [1].

The (k, n) anti-fraud visual cipher scheme is given by S_0^0 , S_0^1 , S_1^0 andS_1^1 4 basis matrices, where the subscript of the basis matrix indicates the color of the shared secret image S, and the superscript indicates the color of the authentication image I. 0 indicates white and 1 indicates black. The sharing rules are shown in Table 1.

Table 1. Anti-fraud visual password scheme sharing rules.

Matrices	Secret Image	Verify Image
S_0^0	white	white
S_0^1	white	black
S_1^0	black	white
S_1^1	black	black

2.1. A Visual Password-Sharing Scheme That Prevents Spoofing

Jie Guo, Hao Yan, et al. Propose a visual password scheme that can find out who provides forged sharing spoofers during the recovery process [2].

2.1.1. Spoofer can be found.

The goal of this scheme is to realize both a (k, n) threshold scheme and a (k-1, n) threshold scheme (secret image and authentication image are of the same size) in one sharing process. This is done by constructing a (k, n) threshold visible cipher scheme in which not only k shares can recover the hidden picture I, but also k-1 shares can recover another authentication image I' (I' can be independent of or part of I), and since the spoofers provide forged shares, it will be not be able to recover the hidden picture I and the verification image I', all k-1 combinations of k shares can be tried, and only the combinations that do not contain the deceiver can recover the verification image I', and thus, in the case where only one deceiver exists, it is possible to find out who the deceiver is.

2.1.2. Up to k-1 spoofers can be found.

The goal of this scheme is to discover at most k-1 deceivers using (2, n) and (k, n) thresholds, provided that the verification image I' is public. This is done by sharing the secret image I with the (k, n) threshold and sharing the verification image I' of the same size with the (2, n) threshold, such that any two honest participants can recover the verification image I', and the secret image can be restored by any k sincere participants.

However, this scheme still suffers from the problem of ghosting the verified image in the recovered secret image, which affects the discrimination of the secret image.

2.2. Anti-fraud Visual Cryptography Without Reimaging

Xiaohui Xu and Bin Yu Spoof-proof visual cipher scheme is constructed by original (k, n) and improved (k-1, k-1) visual cipher schemes, which can detect the spoofers and overcome the problem of the existence of the verification image ghosting in the recovered covert picture, and can recognize the secret information more clearly.

The scheme consists of an ordinary visual cryptography scheme with four base matrices satisfying the contrast condition and security condition of visual passwords, as well as the definition of a spoof-proof visual password plan; when the number of participants is less than k-1, the submatrices of these four base matrices are indistinguishable, and the same matrices are able to be obtained by a simple

columnar transformation; when there are k-1 participants, the authentication image is able to be restored, while not get any information about the covert picture; when there are k or more than k participants, the covert information can be restored correctly. The process of detecting the spoofers is as follows: try all the combinations of k-1 participants out of k. Only the combination of k-1 participants that do not contain the spoofers can recover the authentication image I', and the remaining one is the spoofers, and it takes at most $\binom{k}{k-1}$ times, i.e., k times, to find out the spoofers. The execution process is shown in Fig. 1, and the images used in the scheme as well as the simulation results are shown in Figure 1, Figure 2 and Table 2.

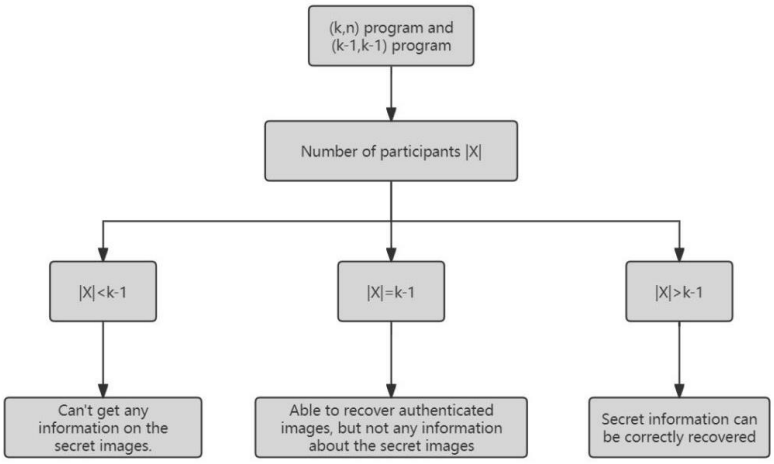


Figure 1. Execution process of anti-fraud visual cryptography without reimaging (Photo credit: Original).

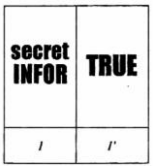
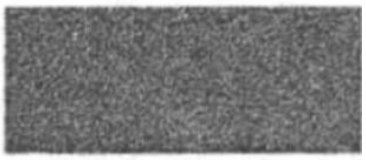
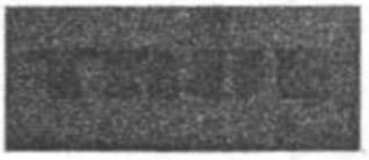


Figure 2. Secret image and authentication image [3].

Table 2. Simulation effect of anti-fraud visual cryptography without reimaging.

Name	Image
Share	
Recovered authentication image	
Recovered secret image	

However, the scheme still does not solve the problem of the presence of multiple spoofers.

2.3. Anti-fraud Visual Cryptography Based on Cumulative Matrix

Yu Bin, Xu Xiaohui et al.错误!未找到引用源。 Multiple independent deceivers among them can be discovered without additional information through the shared copies owned by the participants. Compared with other deception-proof schemes, this scheme is simple to construct and only needs to connect the matrices generated through the cumulative matrices according to the rules to get the base matrices that satisfy the conditions. This system has a high information rate and a relatively tiny pixel extension. Most prominently, the scheme can detect multiple spoofers, which strengthens the anti-spoofing function.

The four base matrices of this scheme are all connected by the ordinary visual password scheme matrix, which satisfies the security condition and contrast condition of visual passwords, and also satisfies the definition of an anti-fraud visual password scheme. When a spoofing agent exists, it can find out the spoofing agent by whether it can recover the verification image, so that its spoofing behavior cannot succeed. Figure 3 depicts the program's execution, and Table 3 displays the outcomes of the simulation.

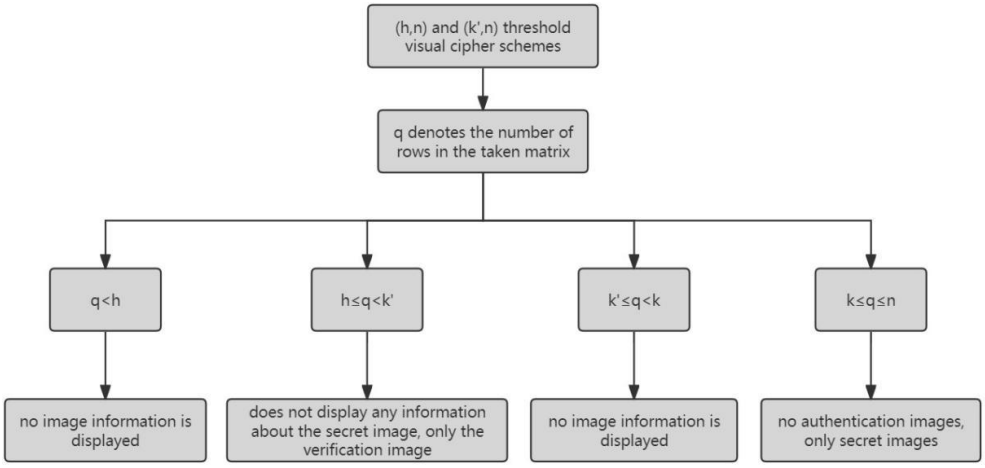
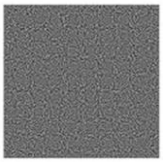


Figure 3. Execution process of anti-fraud visual cryptography based on cumulative matrix (Photo credit: Original).

Table 3. Simulation effect of anti-fraud visual cryptography based on cumulative matrix.

Name	Image
1 shared copy	
2 shared copies	
3 shared copies	
4 shared copies	

While the three solutions described above address the problem of deceptive behavior by participants, there is still the problem of possible deceptive behavior by distributors.

2.4. Anti-fraud Visual Cryptography with Trusted Third Parties

Qingping Mo and Xiaoqing Tan The problem of participant deception is addressed by describing the introduction of a trusted third party (TTP) using (k, n)-VCS. By analyzing the feasibility, performance, and security of the plan, it is concluded that the plan can detect not only third-party deception, but also the deception of multiple participants. Its execution process is shown in Fig. 4.

The central idea of the scheme is that in order to verify whether the sharing of each participant is authorized (i.e., whether the sharing image i1,..., in whether it is modified), he can either verify it with a participant or request verification from the TTP; in order to verify whether the distributor assigns an authorized but forged share to a participant (i.e., whether the share image r1,..., rn whether it is a forgery), a certain number of participants are required to verify with the TTP. The scheme stipulates that each participant must first determine that his/her share is authorized before proceeding to recover the secret image while assuming that the share is secure throughout the distribution process; the loss of the image during the distribution process does not affect the recovery of the image. The scheme is simulated with the selected secret and verification pictures as demonstrated in Fig. 4, and the sharing image generated from the above plan is shown in Fig. 4, depicts one of the two sharing images retained by the TTP, and the image superimposed on it and any of the sharing images of the participants is shown in Figure. 4.

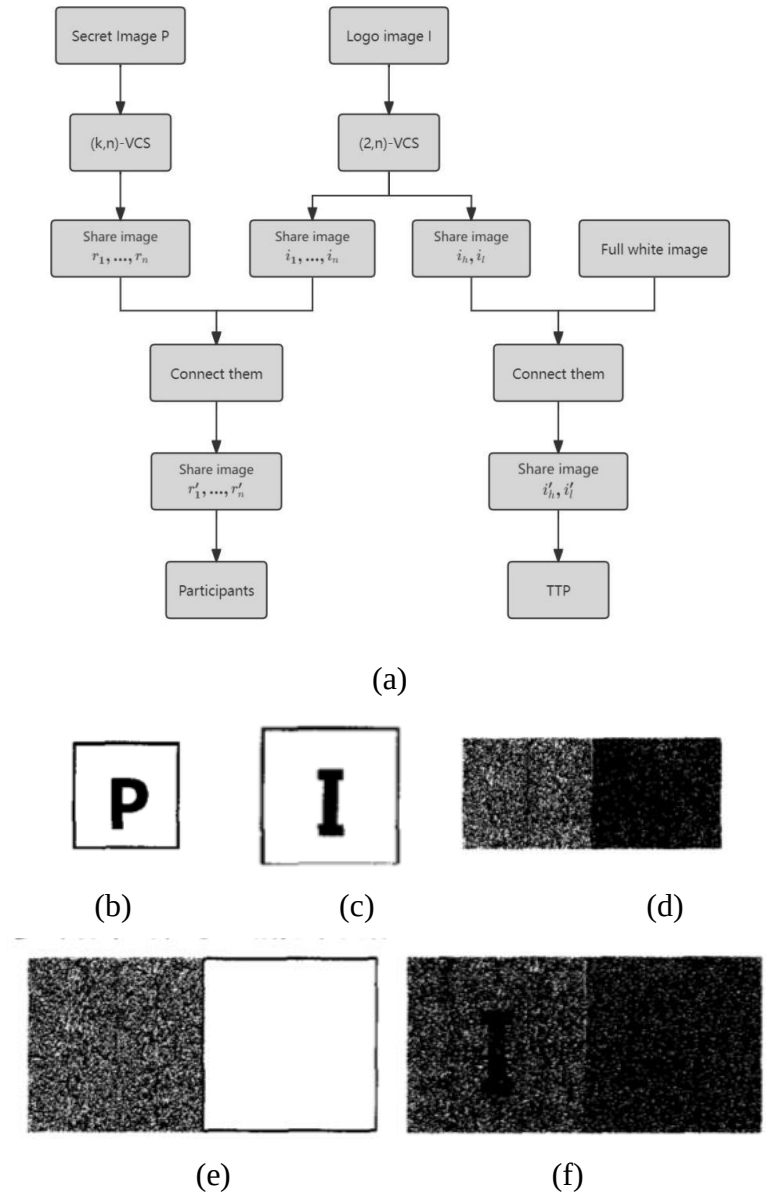


Figure 4. (a) Execution process of anti-fraud visual cryptography with trusted third parties. (b) Secret Image. (c) Logo image. (d) Any shared image. (e) One of the two shared images retained by TTP. (f) Overlay of shared images retained by TTP and any of the shared images from the participants [4].

2.5. An Improved Anti-Fraud Visual Cryptography

Shu Zhang, Wei Li et al. have developed an advanced (2, n+1)-VCS to share verification images without the need for a Trusted Third Party (TTP). Detailed in Figure 5, this method modifies the traditional (k, n)-VCS model by employing an improved (2, n+1)-VCS. In this scheme, the verification sub-share count is increased to n+1, with the additional share designated to assess potential spoofing by participants. Simultaneously, the distributor D retains a validation sub-share, allowing participants to directly verify if the distributor is engaging in spoofing. This approach effectively provides a robust mechanism for testing the authenticity of both participants and distributors without involving a TTP. The application of this scheme is illustrated with the selection of secret and verification images as shown in Figure 5(a). The verification sub-share image Ml, chosen randomly for secure storage by distributor D, is depicted in Figure 5(b). A specific sub-share image obtained by participant Pi (where i=1, 2, 3) is shown in Figure 5(c). The overlay of the sharing image Ml retained by the distributor with one of the participant's images is shown in Figure 5(d). Finally, the superposition of three sharing images Ri (i=1, 2, 3), obtained by participant Pi, is

presented in Figure 5(e). Compared to earlier methods, this scheme offers fewer execution rounds, optimal compatibility and contrast, along with simplicity and feasibility. These improvements enhance the security of both the secret sharing and recovery processes, demonstrating significant practical value..

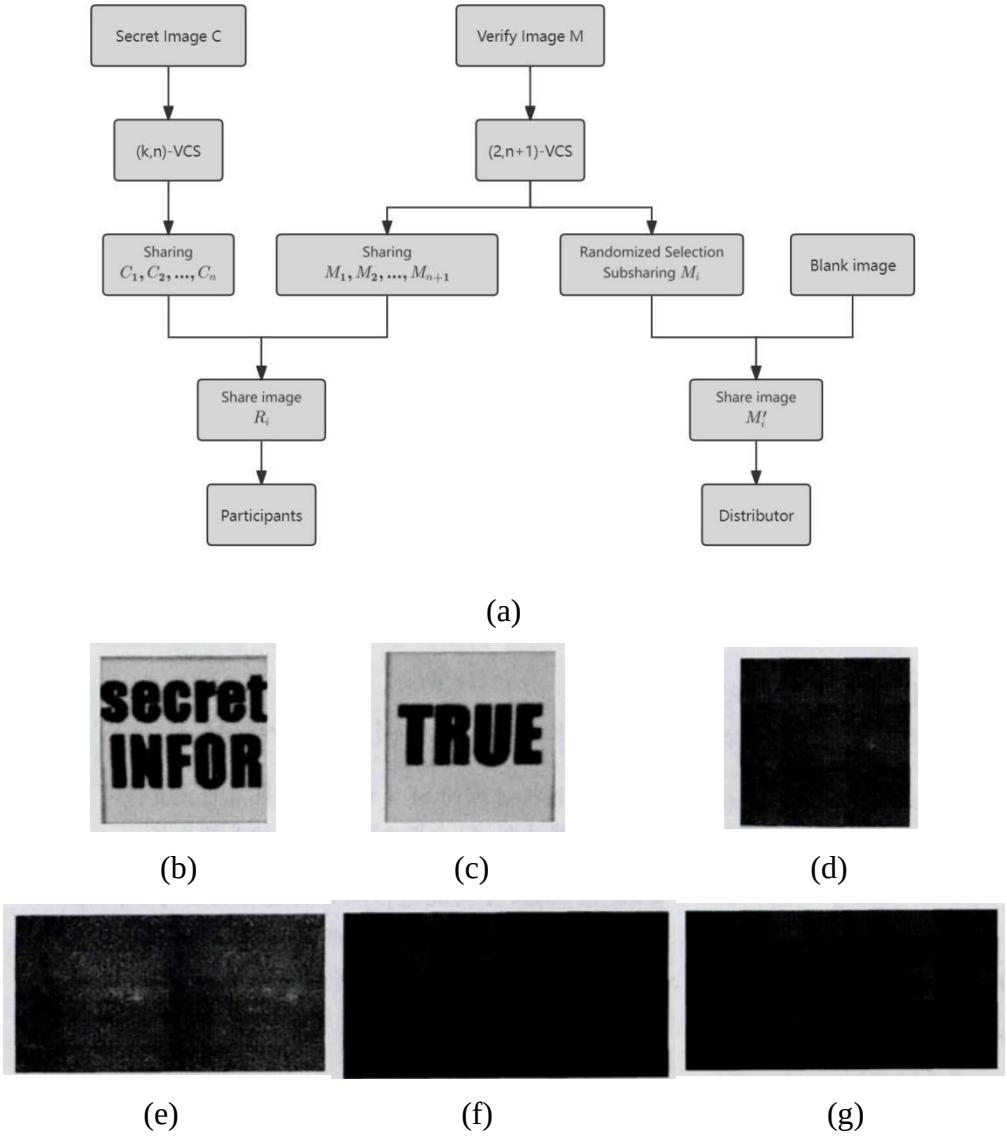


Figure 5. (a) Execution process of an improved anti-fraud visual cryptography错误!未找到引用源。(b) Secret Image错误!未找到引用源。. (c) Verification image. (d) Distributor D randomly selects the verified sub-shares of the custodial. (e) A certain sub-shared image R obtained by participant Pi. (f) Overlay of Mi retained by a distributor with a particular share of Ri. (g) Overlay of the three shared Ri (i=1,2,3) obtained by the participant [5].

The above two schemes not only address the problem of the deceptive behavior of the participants but also the problem of the deceptive behavior of the distributors.

3. Application of Visual Cryptography

3.1. Optimal Visual Password Scheme For Creating Multiple Shares for Multimedia Applications

Since images are the primary interactive media used in multimedia data to communicate visual message to the public, Many hackers try to use illicit methods to gain secret images [6]. As a result, an ECC (Elliptic Curve Cryptography) method based on OGWO (Oppositional Gray Wolf

Optimization) is proposed that sends the original picture to the receiver in a more discreet and private manner [7].

Three stages make up this work's visual encryption: (a) ribbon separation; (b) large-scale share generation; and (c) optimal encryption and decoding. An elliptic curve cryptography algorithm based on OGWO is suggested to realize the encryption and decryption of the picture. The decrypted image is compared to quality parameters like PSNR, MSE, CC, etc. to assess the effectiveness of the suggested method. The outcomes of the suggested method are examined through the use of numerous test images, and it is determined that the scheme is significantly more resilient than traditional encryption techniques.

With greater secrecy and anonymity, the sender can convey the hidden picture to the receiver using this manner.

3.2. QR Code Secure Payment Solution Based on Visual Cryptography

As information technology has advanced, the QR code, as a new information storage and transmission technology, plays a role in many fields, but the traditional QR code is easy to be tampered with, and there are security risks, so based on the visual password technology, a verifiable QR code payment scheme is proposed [8]. Using a pixel-level-based sharing scheme, the QR code and the verified image are split, and one of them is directly encoded to provide a QR code that the user can use, which solves the problem that the scanning device cannot be accurate to the pixel level [9]. Based on this, the pixel points on the shared image are completely randomized, and the attacker cannot tamper with the information based on the separate shared copies. Utilizing the multi-secret visual password scheme, the recovered QR codes are verified to enhance the security of QR codes [10].

Here is the precise procedure: select a verification picture of the same size as the QR code, encrypt it together with the QR code image, and generate two copies of the share, one copy of which is secretly stored in the cloud, and the other copy of which, together with the storage address in the cloud, generates the QR code [11]. Scanners read the QR code to obtain the sharing copy and the cloud address, send the sharing copy to the cloud, and the cloud sends the restored QR code with the verification image back to the user by decrypting the overlay, and the user determines the QR code's security based on the verification image. The process can be represented in Figure.6.

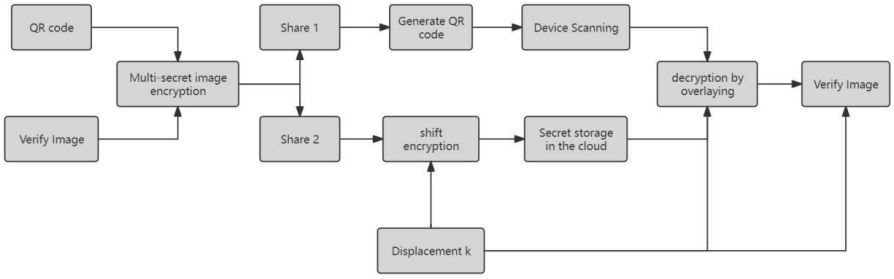


Figure 6. Execution process of QR code secure payment scheme based on visual cryptography [12].

3.3. An Anti-Fraud Medical Case Encryption Scheme Based on Visual Cryptography

As the Internet has grown, cloud computing and other technologies, large data storage, poor reliability, and low efficiency of the traditional medical gradually to the data-intensive, intelligent use of intelligent medical transformation, medical informatization has greatly promoted the development of intelligent medical landing, so propose an anti-spoofing medical record encryption program that is easy to use by the patients and doctors, and contains a complete medical process. In this scheme, medical record information can be encrypted and uploaded to the storage system for sharing, and recovered using visual passwords, which protects the patient's private information from being leaked; using visual password technology can encrypt and decrypt the images of the medical record as well as encrypt and store various types of medical images of the user; and using the picture of the patient's

consultation department and consultation time as the verification image, which is equipped with the function of anti-spoofing [13].

The program involves three main subjects: (1) patients: patients register for consultation, the doctor submit and encrypt medical records after diagnosis, and patients can view their own medical records in the system. (2)Doctor: By diagnosing the patient's condition and getting certain medical information to generate medical records, the patient's medical history is encrypted and stored in the storage system [14]. (3)IPFS: IPFS is a storage system that utilizes distributed hash tables to address the location and data transmission issues, and can be used to store and share many files with high storage capacity and real-time access. Their specific functions can be represented by Figure 7.

The specific process is as follows: first, the patient logs into the system through the account password to register, the doctor logs into the account to view the details of the registration and calls the number for consultation, and generates an electronic medical record according to the patient's condition, and then archives the examination results as well as the diagnosis, which is recorded as the secret image S, and the picture of the consultation department and the time of consultation are used as the verification image S1, which is encrypted at the same time, and generates the two sharing images R1 and R2, which are uploaded to the IPFS distributed storage system for storage. IPFS distributed storage system for storage, and the addresses of the two images returned by IPFS are built into an index table for storage. When access to medical records is required, the doctor can input the password related to himself to retrieve the shared images from IPFS through the index table, and then transfer them to the doctor's end for verification, if the verification is successful, it proves that the medical records are available, and then decrypt the medical records.

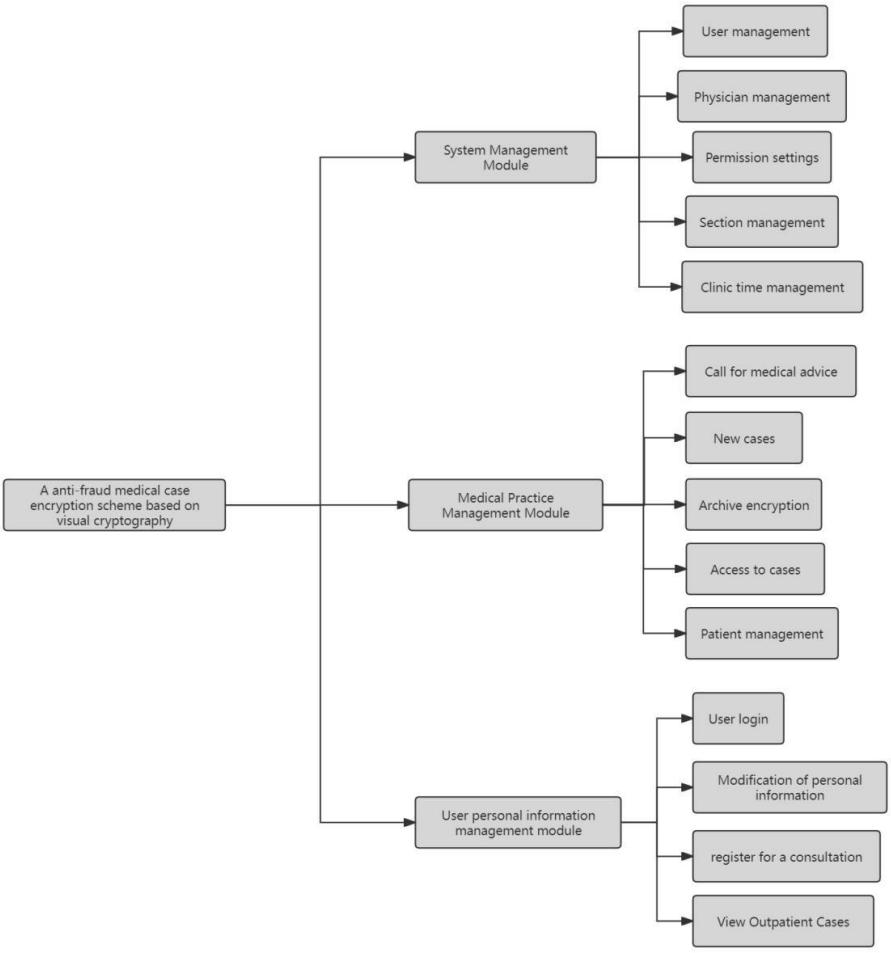


Figure 7. Medical Case Encryption Solution Functional Module [15].

4. Conclusion

Visual cryptography is emerging as a sophisticated approach in information security, offering a novel method for secret-sharing through image processing and coding principles. This technology encodes secret information into multiple, seemingly unrelated sub-images via a specific algorithm, distributing them among participants for safekeeping. The original information can only be reconstructed when a requisite number of sub-images are superimposed by the participants. This decryption method is notably straightforward, requiring no extensive cryptographic knowledge, thereby lowering the barrier to entry. Despite its advantages, visual cryptography faces challenges in practical application. Ensuring users adhere to secure password-setting norms to prevent easy breaches is critical. Moreover, as technological advancements and attack vectors evolve, enhancing the robustness of visual passwords becomes imperative to counteract emerging threats. Looking forward, visual cryptography holds promising applications across various sectors. In healthcare, it can secure patient electronic medical records, ensuring access is restricted to authorized personnel. In finance, it can safeguard customer account information and bolster transaction security. Furthermore, its potential integration into the Internet of Things and big data underscores its importance in securing information transmission and storage.

To advance visual cryptography, efforts should focus on improving user security training, developing more efficient and secure algorithms, and enhancing integration with other security technologies to establish a comprehensive protection system. In summary, visual cryptography offers unique benefits within the domain of information security. Continuing to innovate and expand its applications is crucial for advancing the field's development.

References

[1] M. Naor, A. Shamir, Visual cryptography, Adv. Cryptol.-Eurocrypt'94, Lect. Notes Comput. Sci., vol.950, Springer-Verlag, Berlin (1995) 1-12.

[2] J. Guo, H. Yan, Y. Liu, et al., A cheater detectable visual cryptography scheme, Comput. Eng. (2005) 126-128.

[3] X. Xu, B. Yu, A Cheater Detectable VCS without Fringes, Adv. Comput. Technol. Appl.-2007, Proc. 18th Natl. Acad. Conf. Comput. Technol. Appl. (CACIS), China Instrum. Soc. (CIS), China Soc. Syst. Simul. (CSSS), China Instrum. Soc. Microcomput. Appl. (CACIS), Preparatory Div. Complex Syst. Model. Simul. Comput. Spec. Comm. China Soc. Syst. Simul. (CSSC), Coll. Electron. Technol., PLA Inf. Eng. Univ. (2007) 5.

[4] B. Yu, X. Xu, L. Fang, A cheater detectable VCS based on cumulative array, J. Electron. Inf. 31 (2009) 950-953.

[5] Q.P. Mo, X.Q. Tan, Cheater detectable visual cryptography scheme with third trusted party, Comput. Appl. Res. 28 (2011) 2690-2693.

[6] S. Zhang, W. Li, X. Ai, Improved visual cryptography scheme to prevent cheaters, Comput. Appl. Res. 33 (2016) 3770-3773.

[7] P. Geetha, V. Jayanthi, A. Jayanthi, Optimal Visual Cryptographic Scheme with multiple share creation for Multimedia Applications, Comput. & Secur. 78 (2018) 301-320.

[8] Y. Tan, Z. Li, Secure QRcode payment scheme based visual cryptography, Comput. Digit. Eng. 48 (2020) 2712-2716.

[9] Y. Han, X. Liu, P. Li, An anti-spoofing encryption scheme for medical records based on visual cryptography, J. Beijing Inst. Electron. Sci. Technol. 30 (2022) 19-29.

[10] S. Wan, Y. Lu, X. Yan, et al., Visual Secret Sharing Scheme with (k, n) Threshold Based on QR Codes, 2016 12th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN), IEEE Comput. Soc. (2016) 374-379.

[11] K. Praveen, M. Sethumadhavan, Cheating immune visual cryptographic scheme with reduced pixel expansion, Prog. Adv. Comput. Intell. Eng., Springer, Singapore (2018) 257-265.

[12] X. Zhu, C. Guo, H. Feng, Y. Huang, Y. Feng, X. Wang, R. Wang, A Review of Key Technologies for Emotion Analysis Using Multimodal Information, Cognitive Computation (2024) 1-27.

[13] D.N. Yang, I. Doh, K.J. Chae, Secure medical image-sharing mechanism based on visual cryptography in EHR system, Int. Conf. Adv. Commun. Technol. (ICACT), Piscataway, NJ, IEEE (2018) 463-467.

[14] W.-Y. Wen, Y.-P. Jan, Y.-M. Fang, et al., Authenticatable medical image sharing scheme combined with blockchain, Small Microcomput. Syst. (2021) 1-9.

[15] J. Fu, N. Wang, Y. Cai, Privacy-Preserving in Healthcare Blockchain Systems Based on Lightweight Message Sharing, Sensors (Basel, Switzerland) 20 (2020).