JOURNAL FOR INNOVATIVE DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE

Volume-2,Issue-5 (May-2019)
ISSN (O) :- 2581-6934

Visual Secret Sharing Schemes for QR Code

Ms. M. Sukumari ME [1] , A. Nisha ME [2]

[1] Assistant professor, [2] Student

[1 2] Department of Computer Science and Engineering, Rajas International Institute of Technology for women

Abstract— In this project, a novel visual secret sharing (VSS) scheme for QR code (VSSQR) was proposed with (n, n) threshold based on high capacity, admirable visual effects and popularity of color QR code. By splitting and encoding a secret image into QR codes and then fusing QR codes to generate QR code shares, the scheme can share the secret among a certain number of participants. However, less than n participants cannot reveal any information about the secret. The embedding amount and position of the secret image bits generated by VSS are in the range of the error correction ability of the QR code. On one hand, the secret image can be reconstructed by first decomposing three QR codes from each QR code share.Then stacking the corresponding QR codes based on only human visual system without computational devices. On the other hand, by decomposing three QR codes from each QR code share and then XORing the three QR codes respectively, we can reconstruct the secret image lossless.

Index Terms—Visual secret sharing, general access structures, multiple secrets, information-theoretic security.

INTRODUCTION

1.1 COMPUTER FORENSICS

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

1.2 SECRET SHARING

Secret sharing (also called secret splitting) refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own.

In one type of secret sharing scheme there is one dealer and n players. The dealer gives a share of the secret to the players, but only when specific conditions are fulfilled will the players be able to reconstruct the secret from their shares. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can. Such a system is called a (t, n)-threshold scheme (sometimes it is written as an (n, t)-threshold scheme).

APPLICATIONS OF SECRET SHARING

A secret sharing scheme can secure a secret over multiple servers and remain recoverable despite multiple server failures. The dealer may act as several distinct participants, distributing the shares among the participants. Each share may be stored on a different server, but the dealer can recover the secret even if several servers break

down as long as they can recover at least *t* shares; however, crackers that break into one server would still not know the secret as long as fewer than *t* shares are stored on each server.

This is one of the major concepts behind the Vanish computer project at the University of Washington, where a random key is used to encrypt data, and the key is distributed as a secret

across several nodes in a P2P network. In order to decrypt the message, at least *t* nodes on the network must be accessible; the principle for this particular project being that the number of secret-sharing nodes on the network will decrease naturally over time, therefore causing the secret to eventually *vanish*. However, the network is vulnerable to a Sybil attack, thus making Vanish insecure.

Consequently, although tools and techniques such as Vanish can make data irrecoverable within their own system after a time, it is not possible to force the deletion of data once a malicious user has seen it. This is one of the leading conundrums of Digital Rights Management.

1.3 VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading. One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the ciphertext. Normally, there is an expansion of space requirement in visual cryptography. But if one of the two shares is structured recursively, the efficiency of visual cryptography can be increased to 100%.Some antecedents of visual cryptography are in patents from the 1960s. Other antecedents are in the work on perception and secure communication. Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations.

(2, N) VISUAL CRYPTOGRAPHY SHARING CASE

Sharing a secret with an arbitrary number of people N such that at least 2 of them are required to decode the secret is one form of the visual secret sharing scheme presented by Moni Naor and Adi Shamir in 1994. In this scheme secret image which is encoded into N shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

Every pixel from the secret image is encoded into multiple subpixels in each share image using a matrix to determine the color of the pixels. In the (2,N) case a white pixel in the secret image is encoded using a matrix from the following set, where each row gives the subpixel pattern for one of the components. For instance in the (2,2) sharing case (the secret is split into 2 shares and both shares are required to decode the secret complementary matrices to share a black pixel and identical matrices to share a white pixel was used. Stacking the shares the user has all the subpixels associated with the black pixel now black while 50% of the subpixels associated with the white pixel remain white.

1.4 OVERVIEW OF THE PROJECT

The secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret.

2 SYSTEM ANALYSIS

2.1 EXISTING SYSTEM

An extended visual cryptography scheme (EVCS), for an access structure (rQual; rForb) on a set of n participants, is a technique to encode n images in such a way that when stack together the transparencies associated to participants in any set X єrQual get the secret message with no trace of the original images, but any X єrForb has no information on the shared image. Moreover, after the original images are encoded they are still meaningful, that is, any user will recognize the image on his transparency. The main contributions of the proposed system are the following: A trade-off between the contrast of the reconstructed image and the contrast of the image one ach transparency for (k; k)-threshold EVCS (in a (k; k)-threshold EVCS the image is visible if and only if k transparencies are stacked together). This yields a necessary and sufficient

ISSN:-2581-6934|www.jidps.com

condition for the existence of (k; k)-threshold EVCS for the values of such contrasts. In case a scheme exists explicitly construct it. A general technique to implement EVCS, which uses hypergraph colourings. This technique yields (k; k)-threshold EVCS which are optimal with respect to the pixel expansion. Finally, some applications are discussed for this technique to various interesting classes of access structures by using relevant results from the theory of hypergraph colourings.

2.1.1 DISADVANTAGES

- Less security
- High complexity
- Slow transmission
- Time consumption is more

2.2 PROPOSED SYSTEM

The aim of the proposed system is to maximize the range of the access control of VSS schemes encrypting multiple images. As a first step, the preliminary version maximally generalized the formulations of access structures and VSS schemes for multiple secrets, and then provided a construction of VSS schemes of the most general form. This project provides further developments of this generalization. First, this project justifies the above construction in a more general framework. More precisely, this project introduces a more general construction which includes the previous one as a special case. In particular, this inclusion is strict in the sense that the former (Construction 11) can generate VSS schemes with strictly better contrast and pixel expansion than the latter. Then, this project proves that for any given access structure of the most general form, the former indeed generates a VSS scheme realizing the access structure and also the latter is a special case of the former this completes the justification of the latter construction. Here, to describe the former construction, the proposed system has introduced two notions which together with the proofs to characterize and justify the construction reveal a sufficient condition to be satisfied by the encryption of VSS schemes for multiple secrets. Moreover, it is demonstrated that for threshold access structures, the latter construction generates VSS schemes with the same pixel expansion as (k, n, s)-MVCS and (k, n, s, R)-MVCS. Finally, the optimality of the former (more general) construction is examined, giving that there exist access structures for which it generates no optimal VSS schemes.

2.2.2 ADVANTAGES

- Avoid leakage of information
- Better access structure
- High security
- Fast transmission of visual secrets in images

Here, the sets of the qualified combinations and the forbidden combinations are called a qualified set and a forbidden set, respectively, and the pair of the qualified and forbidden sets is called an access structure. A typical example of SS schemes is the *(k, n)*-threshold SS scheme, in which a secret is encrypted into *n* shares so that any *k* or more shares can reconstruct the secret, while any $k-1$ or less shares leak no information about the secret. In contrast to the ordinary cryptosystems, there exist SS schemes whose decryption can be performed by humans without any numerical computations.

The visual secret sharing (VSS) scheme is an example of such SS schemes. This scheme encrypts a visual secret into visual shares so that humans can visually reconstruct the secret with their eyes by superposing a qualified combination of visual shares each printed on a transparency. One of the applications in which VSS schemes are essential is for the authentication by a human recipient without any trusted communication channels. More precisely, the problem here is to authenticate a message from an informant to a human recipient through an insecure channel which is under full control of an adversary. This arises, for example, in the interactions between a human and an electronic device without screen such as a smartcard. It is hard to provide a solution to this problem without assuming a secure channel and the authentication based on VSS schemes, called the visual authentication has been the only secure solution.

3.SYSTEM DESIGN

Systems design is the process of defining the architecture, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. It involves the identification of classes their relationship as well as their collaboration.

ISSN:-2581-6934|www.jidps.com

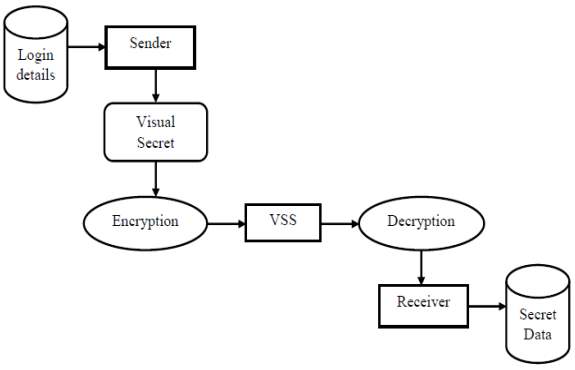

Fig 3.1.1 System Architecture

In this figure 3.1.1, it shows that the access structure was generated to obtain the secret image then the accurate condition was provided to perform the encryption and the threshold access structure was applied to generate the no optimal solution.

4.SYSTEM IMPLEMENTATION

4.1.1 FORMULATION OF ACCESS STRUCTURE

The formulation of visual sharing scheme was provided by encrypting multiple images. That is the secret image is splited and it is encrypted in the form of multiple images it was formed by having two matrix for describing the security and construction of VSS. Let S = {s1, s2, · · · ,sn} be an ordered set of size n, and a be an ordered subset of S of size n_. For an n_ ×m matrix M = (mi j), let [M]a denote the n × m matrix defined by ([M]a)i j =_mod a (si) j if si∈ a, 1 otherwise.

The matrix [M]a is called the super matrix of M with respect to a. For an n×m matrix M = (mi j), let [M]a denote the n_×m submatrix of M defined by ([M]a)orda(si) j = mi j for si∈ a. The matrix [M]a is called the submatrix of M with respect to a. The submatrix with respect to the empty set ∅ is defined to be the empty string ε; i.e. [M]∅ = ε for all M. Access Structure for Multiple Secrets was given as Let S be a finite set, and q ∈ N. For i∈ [q], let AiQ and AiF be subsets of 2S such that AiQ∩ AiF= ∅. The pairs rq of the subsets AiQ and AiF = r (AiQ ,AiF)i=1, is called an access structure on S for q secrets if AiQ and AiF satisfy the monotonicity .Then the theequivalenmce between the two structures are generated.

4.1.2 VSS SCHEME

In the VSS schemes, the secrets and shares are both visual, and their decryption can visually be performed by human eyes. Each black-white pixel in a secret image is encrypted into a set of black-white subpixels in shares. Hence, the encryption of each pixel can be represented as a pair of matrices *Cb= (Cbij)*with $b \in \{0, 1\}$, where $b = 0$ for a white pixel in a secret image and $b = 1$ otherwise, and $Cbi\,j = 0$ for a white j -th subpixel in the i-th share and $Cbi\,j = 1$ otherwise. A secret image is encrypted into two shares. Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand, the secret image can be reconstructed when both of the shares are superposed. This can be constructed as follows.

A pixel e in the secret image is encrypted into two subpixels in each of the two shares. If e is white (resp. black). The superposition of the two shares has one black subpixel and one white subpixel (resp. two black subpixels) if e is white (resp. black). This construction can be represented by the sets $C0$ and $C1$ of matrices more precisely, the above encryption and decryption can be represented by the functions Enc : {0, 1} → {0, 1}2×2 and Dec : {0, 1}2×2 → {0, 1}2 given by Enc*(b)* = *CbU*and Dec*(M)* = *(m*11 ∨*m*21,*m*12 ∨*m*22*)* for $b \in \{0, 1\}$ and $M = (mi\ j) \in \{0, 1\}2\times2$, respectively, where ∨ denotes the OR operation.

4.1.3 PIXEL EXPANSION

The relative difference in gray level between superposed shares that come from a white pixel and a black pixel in the secret image is called the contrast. In the above example, the reconstructed pixel has a gray level of 2/2 = 1 if e is black, and a gray level of 1/2 if e is white; therefore, Contrast = 2/2−1/2= ½. The higher contrast makes it easier to recognize reconstructed images. The number of subpixels in shares encrypted from a pixel in a secret is called the pixel expansion.

In the above example, a pixel in a secret is encrypted into two subpixels in shares; therefore, Pixel expansion = 2. The lower pixel expansion allows the more practical resolution of share images. A VSS scheme and its encryption are called optimal if they have the lowest pixel expansion.

ISSN:-2581-6934|www.jidps.com

4.1.4 DECRYPTION

In general, it is difficult to examine the optimality of SS schemes realizing a general access structure in fact, the optimality has been shown so far only for very limited classes of SS schemes such as threshold SS schemes threshold VSS schemes and (non-perfect) uniform SS schemes. Hence, instead of directly examining the optimality, examine the possibility that the optimality of Construction may be reduced to that of each encryption Enc*i*. For this purpose, consider first a simple access structure = *(AiQ, AiF)*∈*i*=1 on *S* = {*s*1, *s*2} for 2 secrets,. This access structure can be realized by a VSS scheme with the (deterministic) encryption given by Enc*(b)* = *b*1*b*2 for *b* ∈ {0, 1}, while any VSS scheme generated by Construction has the pixel expansion no less than 2. Note that the above matrix is the concatenation of the basis matrices *Cb*11,1 and *Cb*21,1 with respect to the row (not column). Then construct an optimal VSS scheme realizing *by* defining its encryption to be the concatenation of {Enc_*i*}*i*with respect to the row . Hence the optimal pixel expansion for _ is max*i mi* and it generates the no optimal VSS scheme. The recipient retrieves the secret information from the encrypted multiple images by decryption. Decryption is done by superimposing the n shares.

CONCLUSION

This project provides an application of our VSS schemes. In the authentication based on VSS schemes encrypting a single secret image, one way to detect tampering by an adversary is to divide the secret image into two disjoint areas: one for a message and the other for the detection. On the other hand, VSS schemes encrypting multiple images allow the authentication in which Shares 1 and 3 are distributed to a human recipient, Share is generated by an informant, and the two secrets *v*1 and *v*2 are taken to be an all-black image for the detection and an image for a message, respectively. This authentication, equipped with the idea behind the third method "black and gray" in ensures that an adversary cannot tamper with the latter image without tampering with the former, which makes its security analysis simpler and more practical.

FUTURE ENHANCEMENT

This project can be further modified in future to investigate this authentication more in detail. In the Proposed work the visual secret data's are send directly to the receiver, this can be modified by sending the secret visual data's to the cloud and then to the recipient.

REFERENCES

[1]. C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson (2003), "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261

[2]. Y.-C. Chen (2017), "Fully incrementing visual cryptography from a succinct non-monotonic structure," IEEE Trans. Inf. Forensics Security, vol. 12, no. 5, pp. 1082–1091.

[3]. S. Cimato, R. de Prisco, and A. de Santis (2005), "Optimal colored threshold visual cryptography schemes," Des., Codes Cryptogr., vol. 35, no. 3, pp. 311–335.

[4]. Y. Desmedt, S. Hou, and J.-J. Quisquater (1998), "Audio and optical cryptography," in Advances in Cryptology—ASIACRYPT (Lecture Notes in Computer Science), vol. 1514. Berlin, Germany: Springer-Verlag, pp. 392–404.

[5]. M. Naor and B. Pinkas, "Visual authentication and identification," in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 1294. Berlin, Germany: Springer-Verlag, 1997, pp. 322–336.

[6]. M. Sasaki and Y. Watanabe (2014), "Formulation of visual secret sharing schemes encrypting multiple images," in Proc. 39th IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), pp. 7391–7395.

[7]. S. J. Shyu (2014), "Threshold visual cryptographic scheme with meaningful shares," IEEE Signal Process. Lett., vol. 21, no. 12, pp. 1521–1525.

[8]. S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen(2007), "Sharing multiple secrets in visual cryptography," Pattern Recognit., vol. 40, no. 12, pp. 3633–3651.

[9]. R. Z. Wang (2009), "Region incrementing visual cryptography," IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662.

[10]. C.-N. Yang and T.-H. Chung (2010), "A general multi-secret visual cryptography scheme," Opt. Commun., vol. 283, no. 24, pp. 4949–4962