ORIGINAL RESEARCH PAPER
VOLUME-6 | ISSUE-6 | JUNE-2017 | ISSN No 2277 - 8179 | IF : 4.176 | IC Value : 78.46
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

Visual Cryptography Schemes for the Generation of Secret Share Generation for Information Hiding

Computer Science

Ranjan Kumar M.Tech. Scholar, CSE Department, IES college of Technology, RGPV Bhopal, India
Aishwarya Mishra Associate Professor, CSE Department, IES college of Technology, RGPV Bhopal, India

ABSTRACT

the current decade of information sharing over the internet faced a problem of security threats and man in middle attack. For the prevention of attacks and security threats used various cryptography techniques. The cryptography technique provides better security strength of information hiding, but cannot detect the attacker path and the integrity of cracked data. Now a day used another security measure concern is called visual cryptography for the generation of share. The generation of share proceeds in terms of block information over the internet. In this paper present the review of visual cryptography based on different technique for the generation of share.

KEYWORDS:

Visual Cryptography, Share Generation, Encryption, Key Generation, Image

INTRODUCTION

A visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into n noise-like shares. The secret image can be decrypted by the human eye when any k or more shares are stacked together [11][12]. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the share-images are larger than the original secret image. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry. Since the concept of visual cryptography was first proposed, there have been several studies making efforts to deal with the pixel expansion problem [2,11]. Most of these have fallen into the category of probability visual cryptography schemes. An encryption algorithm is proposed to hide the shared pixels in the single image random dot stereogram's (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this paper tries to use SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. Visual Secret sharing (VSS), which is also called visual cryptography (VC), is a technique of cryptography which prevents a secret from being modified or destructed by using the notions of perfect cipher and human visual system. For a general scheme of (k, n) threshold, a secret image is encrypted into n random-looking images, also called shares or shadows. These n shares are then distributed to n associated participants. To visually reveal the secret, any k or more shares are required to stack together. But any k or fewer shadows give no clue about secret. Compared with some conventional encryptions such as DES and AES, VSS offers unbreakable encryption if a meaningless share contains truly random pixels such that it be a one-time pad system[7][8]. Without using a computational device and crypto-graphic knowledge in decryption, VSS technique is effective and suitable for certain practical applications. In section II. Discuss the related work and in section III discuss problem formulation. In section IV discuss approach of visual cryptography result and finally discuss conclusion and future work in section V.

RELATED WORK

In this section discuss the related work in the fields of visual cryptography for the generation of share for the hiding the information. The various authors proposed the various algorithms for the generation of share based on random number generation and correlation of coordinates for the processing of image in from of share.

Problem Formulation

In this section discuss the problem related to share generation using visual cryptography. The generation of share faced a problem of number generation and randomization of number for the process of coordinate's generation. Proactive secret sharing scheme can be used in Public Key Infrastructure (PKI) schemes where Certificate Authority (CA) is used to generate digital signatures. The digital certificate contains a public key, digital signature and identity of the owner of the certificate [4][5]. In such key management applications, our scheme can be applied. CA has a private key for generating digital signatures. Instead of storing the entire key secretly, it is better to divide the key into number of shares and share the key. This private key can be stored as a secret; and is shared in a secret sharing scheme. Once if all the private shares are able to recover the master secret, then the secret is no longer secure. So it is necessary to renew the master secret keeping all the private shares secure [13][14]. If all the private shares are kept secure during secret reconstruction, dealer only needs to renew master secret but not the private shares. So in this way, the secret sharing scheme becomes even more efficient as the private shares can be reused for a longer period of time. If once the shareholders are able to recover the master secret, then the secret is no longer secure. So it is necessary to refresh both the shares and secret at the same time. The future work could be to incorporate both secret and share refreshment together in a complete key management systems[8].One of the limitations of proactive secret scheme is that they assume the set of shareholders remain same forever. The proactive secret sharing scheme could further be extended in adding and deleting shareholders while sharing the same secret [5].

Approach Used

Secret sharing schemes protect the secrecy and integrity of information by distributing the information over different locations. The (*t, n)* threshold secret sharing schemes were introduced by Shamir and Blakley independently in 1979 for protecting the cryptographic keys. Generation of shares and reconstruction of shares are challenging task in cheaters scenario. Cheaters identification is critical task on the time of share reconstruction. In this dissertation we proposed a roust secret share generation technique such technique based on cyclic point intersection of langrage's interpolation[8]. In the process of share generation, construction and cheater identification, we proposed four steps. (i) Cyclic share generation (ii) share reconstruction and (iii) cheater identification. The proposed scheme used some notations are defined we assume that P is a participant set that contain n participant p1, p2, p3…….pn. Such that p= {p1,p2,p3,…….pn} and c1,c2 …cn are cyclic prefix of interpolation equation. Each member of P shares a secret K and hold a secret cyclic prefix Ci where 1≤i≤n.

Share generation phase.

Assume that a dealer wants to share a secret K among the n members in P. First, the dealer specifies the threshold value t freely within the range $1 \le t \le n$. then dealer select three point of prime in subsequent in cyclic x ,y, z [3].

The dealer randomly generates n different polynomials fi's of degree t−1, such that

$$Fi(X) = a(i,0) + a(i,1)X + \cdots\ldots\ldots\ldots + a(i,t-1)Xt$$

Now then the cyclic point of intersection put into each generated shares Xc, Yc and Zc

As
Consider two distinct points J and K such that J = (xcJ, ycJ) and K =

(xcK, ycK)
Let L = J + K where L = (xcL, ycL), then
xcL = s2 - xcJ – xcK
yL = -yJ + s (xJ – xL)
s = (yJ – yK)/(xJ – xK), s is the slope of the line through J and K.

If K = -J i.e. K = (xJ, -yJ) then J + K = O. where O is the point at infinity.
If K = J then J + K = 2J then point doubling equations are used.

Then dealers send the all generated shares to participant.

The Secret Reconstruction Phase
Assume that the participants P1, P2. Pr of any qualified subset in P wants to Cooperate to reconstruct the shared secret K. They can perform the following steps To determine the shared secret K. In the reconstruction phase we apply cyclic addition point of interpolation[5].

Consider a point J such that J = (xcJ, ycJ), where $yJ \neq 0$
Let L = 2J where L = (xcL, ycL), Then
xcL = s2 – 2xJ mod p
ycL = -ycJ + s(xcJ - xcL) modZc
s = (3xcJ 2 + a) / (2yJ) mod Zc, s is the tangent at point J and a is one of the parameters

Chosen with the elliptic curve. If yJ = 0 then 2J = O, where O is the point at infinity.

CONCLUSIONS

In this paper present the review of visual cryptography for the generation of share using image data. The generation of share used text data as well as image data. The generation of share faced a problem of length of share and exchange of coordinate for the processing of share generation. The generation of share take more time, the maximum time of share generation gives the more time for man in middle attack. The key length of share is also major issue. In visual cryptography process the major terms is cheater detection. The process of cheater induces the fake share in the time of share merging. In future used the cyclic key technique for the visual share generation. The proposed method reduces the security risk of share generation.

ACKNOWLEDGEMENT:

First of all I would like to thank my thesis guide Aishwarya Mishra, Associate Professor, CSE Deptt., IES college of Technology, Bhopal. The door to Prof. Mishra office was always open whenever I ran into a trouble spot or had a question about my research or writing. She consistently allowed this paper to be my own work, but steered me in the right direction whenever she thought I needed it. I am also thankful to my HOD, CSE Department Mr. Harsh Mathur and all faculty members for their support.

REFERENCES:

[1] Biswapati Jana, MadhumitaMallick, ParthaChowdhuri and Shyamal Kumar Mondal "Cheating Prevention in Visual Cryptography using Steganographic Scheme", IEEE, 2014, Pp 706-712.
[2] Pallavi Vijay Chavan, Dr. Mohammad Atique and Dr. Latesh Malik "Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares", IJNSA, 2014, Pp 91-102.
[3] Ms. Pradnya S. Nagdive and Prof. Anjali B. Raut "Image Visual Cryptography By Using Haar Wavelet Based Decomposition", IJARCET, 2015, Pp 1261-1265.
[4] RengarajanAmirtharajan, SumaiyaSulthana, P. ShanmugaPriya, G. Revathi, A. Kingsly Infant and J.B.B. Rayappan "Seeable visual but not sure of it - A visual cryptographic perspective for TAMIL characters", IJET, 2013, Pp 1-9.
[5] DoshiRuchali, Kale PrajaktaandPasalkarPranoti "Secured Transaction System Using Steganography and Visual Cryptography", IJESC, 2016, Pp 5542-5546.
[6] SmitaPatil and Jyoti Rao "Survey of Cheating Prevention Techniques in Visual Cryptography", IJSR, 2014, Pp 560-563.
[7] K.S.Suganya and K.Manikandan "Enhanced Secure E-Gateway using Hierarchical Visual Cryptography", IJTET, 2015, Pp 13-17.
[8] L Jani Anbarasi, Modigari NarendraandAnandha Mala G.s "Cheating Prevention using Genetic Feature Based Keyin Secret Sharing Schemes", Communications in Computer and Information Science, 2014, Pp 1-9.
[9] BiswapatiJana,GargiHait and Shyamal Kumar Mondal "Survey on Size Invariant Visual Cryptography", IJCSIT, Pp 3985-3990.
[10] SnehaA.DeshmukhandP.B.Sambhare "Survey of Various Techniques on Cheating Prevention in Visual Cryptography with Steganography Scheme", IJSR, 2014, Pp 2425-2428.
[11] PriyaVenny and Jyoti Rao "A Survey on Cheating Prevention with Verifiable Scheme", International Journal of Computer Applications, 2016, Pp 21-25.
[12] Anju Mohan "A New Meaningful Adaptive Region Incrementing Visual Secret Sharing Based on Error Diffusion and Permutation Encoding with Cheating Prevention", IJSR, 2015, Pp 1526-1530.
[13] Mr. K.P. Vignesh Kumar andProf. M. Sivakumar "DATA EMBEDDING METHOD USING VISUAL CRYPTOGRAPHY", IJAICT, 2014, Pp 254-258.
[14] Reshma More, Gajanan Wayal, Neha Thopte, DivyaWalgude, Prof N.J. Kulkarni and Prof S.S Mujgond "A Review on Cheating Identification and Prevention in Secret Sharing Scheme Using Digital Watermarking", International Journal of Emerging Engineering Research and Technology, 2014, Pp 253-259.