International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 1 Issue 5, September 2014

# VISUAL INNOVATION TOWARDS SECURE ENVIRONMENT

*Dr.S.Nirmala[1], A.Alif Siddiqua Begum[2]*
*Principal[1], Research scholar[2],*
*Muthayammal Engineering College, Rasipuram[1], Al-Ameen Engineering College, Erode[2]*
*nirmala.ramkamal@gmail.com[1], alifsiddi@gmail.com[2]*

***ABSTRACT***

*Visual Cryptography (VC) is novel technique where one secret can be divided into two or more shares. These shares on transparencies when superimposed exactly together, the original secret can be recovered without computer aid. In this article visual cryptography approach is defined and some crypto graphical solutions from literature are discussed, recent research in the field of visual security is reviewed, including visual cryptography technique, and a comprehensive survey of cryptographic literature which applies these procedure to date. The concept of visual cryptography model which serves to aid in interpretation of contrast and security property is also presented.*

***KEYWORDS***

*Visual cryptography, visualization, secret sharing, security, parties' authorization.*

## 1.INTRODUCTION

With technological advancement and increased digitalization of personal data there has been more and more emphasis on data security. Protection of this data in a safe and secure manner does not hinder the access of an authorized authority leading to very difficult and interesting research problem. Thus cryptographic communities have made many attempts to solve this problem. Fortunately visual cryptography allows us to effectively and efficiently share secrets between a large numbers of trusted parties. As trust with many cryptographic schemes is the most difficult part. The first visual cryptographic technique was developed by Moni Naor & Adi Shamir in 1994. It involved breaking up the image into n shares, so that only someone holding n shares could recover the image by overlaying each of the shares over each other. Practically, this can be done by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. To begin visual cryptography is used for encryption of visual information in a secure manner such that decryption is performed by human visual system.

## 2. VISUAL SECURITY

As more and more service are offered to private and corporate users the possible privacy consequences are normally not taken into account w.r.t issues namely awareness and usability. Fortunately Confidentiality as a Service (CaaS) paradigm provide usable confidentiality and integrity for most users, for whom the current security mechanisms either require too much effort or too complex. The paradigm integrates data security with design usability, and combines the same into available cloud service applications and workflows. The splitting of trust is leveraged between cloud service providers and CaaS providers in order to improve usability. CaaS concentrates on unobtrusive confidentiality by hiding all cryptographic artifacts from non-technical users. Here symmetric encryption and invisible key management provides data protection[1]. With the rapid use of visual media in practically all areas of applications including e-commerce/mcommerce, security has become one of the major concerns while sending secret information. Visual Secret Sharing Scheme(VSSS) enables encryption of secret into meaningless share image so that information can be revealed by human visual system (HVS) without using any device or complex mechanism. Most of the existing visual secret sharing schemes involve pixel expansion that increases the memory requirement and communication time. Approach of visual encryption that does not require pixel expansion, however suffers from problem of low contrast after decryption which makes it difficult for HVS to deciper. Hence a VSSS that produce high constrast images after decryption makes it easier for HVS to reveal the information. It also minimizes the communication time and memory requirement while producing better quality decryption for HVS[2]. To support Role Engineering decisions and Role-Based Access Control(RBAC) Visual Role Mining is presented. Its role engineering approach graphical user-permission assignments enable quick study and elicitation of major roles. Here two Algorithms are introduced ADVISER & EXTRACT. ADVISER - heuristic represent user-permission assignments. EXTRACT - probabilistic algorithm used with ADVISER for a visual elicitation of roles [3]. A challenge for information technology in the field of assuring confidentiality of keys and parties authorization now-a-day is to build public key infrastructure and advanced encryption algorithm based on crypto biometric keys. Such keys, apart from their cryptographic characteristics, are also personalized and contain information characterizing their owners. Thus a new technique for generating crypto biometric keys based on unique biomedical images and hashing abbreviating functions is presented [4]. To design, verify and implement security protocol graphical models are combined with

International Journal On Engineering Technology and Sciences – IJETS™
ISSN (P): 2349-3968, ISSN (O): 2349-3976
Volume 1 Issue 5, September 2014

rigorous formal methods. Domain-specific abstraction keep graphical models simple, yet powerful enough for complex, realistic protocols[5]. Visual component architecture for Security Information and Event Management (SIEM) system help to comprehend large amount of security data. Visualization is essential part of the SIEM system. The architecture uses different visualization technologies at the same time extending application functionality. Illustrate GUI of attack modelling component. To increase efficiency of visualization techniques principles of human information perception and interaction issues applied when designing graphical components[6]. To manage security aspects in enterprise-level application and assist programmers in coding access control for java application VICOMS framework is used. It has been embedded within the edipse open source integrated development environment and used experimentally in several case studies[7].

**3.VISUAL CRYPTOGRAPHY(VC) TECHNIQUE**

**Working of VC:**

VC in its simplest form (access structure (2,2) – threshold VC) takes a secret image and encrypts it into two different shares that reveals secret image when they are overlaid. Therefore additional information required to create this kind of access structure is not necessary. Figure 1. explains the working of VC, where VE represent visual encryption and HD represent human decryption w.r.t overlaid shares.

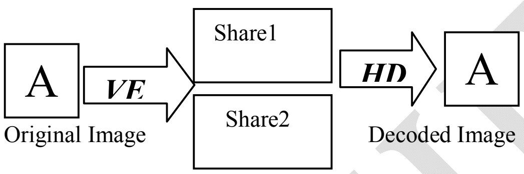


Figure 1: Working model of VC

The general access structure (k,n) threshold for this scheme encodes the secret image into n shares such that when any group of at-least k shares are overlaid the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

**Model for VC:**

Here VC model as well as (k,n) – threshold VC scheme that was proposed by Naor and Shamir are discussed.

Hamming-weight:

In symbol representation hamming weight is number of non-zero symbols in a symbol sequence. In binary representation its the number of "1" bits.

OR-ed k-vector:

Given j×k matrix its k-vector where each tuple consists of result of Boolean OR on its corresponding column vector j×1.

6-tuple(n,m,s,v,α,d) :

An VC scheme is a 6-tuple (n,m,s,v,α,d). Each pixel appears in n versions, one for each transparency representing shares. Each share is m black and white subpixels collection. The resulting structure illustrated by an n×m Boolean matrix $S=[S_{ij}]$ where $S_{ij}=1$ iff the $j^{th}$ subpixel in the $i^{th}$ share is black. Therefore, the gray level of combined share is propostional to OR-ed m vector Vs Hamming weight H(V). This grey level indicate black if $H(V) \geq d$ and white if $H(V) < d-\alpha m$ for some fixed threshold $1 \leq d \leq m$ and relative difference $\alpha > 0$. $\alpha m$, the difference between minimum H(V) value of black pixel and maximum allowed H(V) value for a white pixel is called the contrast of VC scheme.

**VC Property :**

A subset in VC is qualified if and only if its cardinality is k, are called (k,n)-threshold VC. Construction to (k,n)-threshold VC consists of two collections(C0 and C1) of n×m Boolean matrices, each with size r. Construction of b & w pixel require C1 & C0 respectively. The chosen matrix will define color of m sub pixels in each one of the n transparencies. For a valid solution three conditions are necessary, namely:

[i]. For any matrix S in C0, the "or" operation satisfies $H(V)<d-\alpha m$.

[ii]. For any matrix S in C1, the "or" operation satisfies $H(V)\geq d$.

[iii].For any q×n matrices, such that S0 є B0 and S1 є B1 are identical up to column permutation.

Constract is stated by condition first and second of VC. The third condition states the security property of (k,n) threshold VC. One cannot gain any hint in deciding the color of pixel, regardless having any amount of computation resources if have not been given k shares of secret image.

**VC Technique:**

According to theory stated by Noar and Shamir a secret black-white image can be encrypted into shares using Visual Cryptography Scheme(VCS). Without any cryptographic computation qualified group of participants can recover the secret. Unfortunately malicious group can corrupt the traditional scheme. As a solution to above stated problem digital watermarking based verification introduced. This is done without additional cryptographic computation. Every participants using watermark extraction operation to validate other participants shares. Thus security of VCS is enhanced[8]. The property of general k-out-of-n VC present an efficient method for construction of shares based on pre-formed shares. This method applies for authentication and cheater detection[9]. Halftone visual cryptography (HVC) represent visual sharing. Here secret image encoded into halftone shares represent meaningful visual information. HVC encrypts a secret halftone image into color halftone shares. The secret image is embedded into color halftone shares that are constrained by vector error diffusion. This method generate halftone shares showing high quality natural color images[10]. Color visual cryptography scheme is based on modified visual cryptography. This scheme can share a color secret image over a noisy share image and n-1 arbitrary natural images. The encryption process extracts feature images from each natural image, thereby reducing transmission risk, management problems, and pixel expansion problem[11]. Application of VC, Wavelet tree, Integer wavelet transforms and YCbCr color model on color images presents a multi-watermarking scheme. Experimentally all owners hold dual watermark authentication embedded in a protected color images, and at same time the number of ownerships can be increased without re-computing[12].

Image Hatching technique represent non photorealistic line-art. Application such as printing, engraving of currency uses this technique. Brush stroke with diverse styles adopted create aesthetically pleasing textures and shading. Because these types of images has no continuous tone a multilevel scheme is introduced, with different textures based on a threshold level. These textures that apply to different levels are combined to build final hatched image. When secret hidden using vc within hatched image original secret can be recovered without computation. Comparison between original grayscale images and resulting hatched images reinforces the overall quality of hatched scheme. Structural Similarity index (SSIM) is used to perform this comparison[13].

**4.APPLICATION**

With technology advances rapid growing applications on smart phones have provided an excellent platform for mobile visual search. Traditional visual search systems adopt the framework of "Bag of Words", where words indicate quantized codes of visual features. In visual search system based on "Bag of Hash Bits" (BoHB) encodes each local feature to a very small number of hash bits. Instead of quantization whole image is represented as bag of hash bits. BoHB offers benefits in solving mobile visual search issue such as transmission cost, memory cost, etc. BoHB leverage the distinct properties of hash bits for optimized search over gigantic visual databases. This method significantly outperforms CHoG, and other visual search approaches. Boundary feature incorporated at re-ranking step marks object shapes, complementing the local features that characterize the local details. The boundary features can further filter out noisy results and improve the search performance, especially at coarse category level [14]. The evolution of mobile devices introduces new accessibility issues for users with sensory or mobility impairments. For instance, touch screens, lacking tactile cues, are hard to use by blind users without additional feedback. These problems are being mitigated through new interaction paradigms, such as screen readers: software that describe the currently selected elements on the interface through vocal cues[15]. Coming to data security in camera surveillance previous approaches have focused on completely encrypting video stream. To provide secure data Co prime Blurred Pair (CBP) model introduces a spatial encryption that strategically blurs the image/video contents. CPB model create two streams namely public and private by blurring the original video data using two different kernels. Each blurred video stream will provide less access to personally identifiable details for users with lower clearance. For suspicious behavior a supervisor uses both streams to deblur the contents. In CBP theory two kernels when mapped to bivariate polynomials in the Z-domain can be coprimed. Coprimality can be derived in terms of rank of Be'zout matrix formed by sampled polynomials, and an algorithm to factor the Be'zout matrix for recovering the latent image. This scheme effectively protect sensitive identity information in surveillance video[16]. For emergency medical support system with electronic triage tag (eTriage) facilitates emergency medical technicians to grasp patients details through visualization. This system introduces three views of the patients' information namely, Inter-site View, Intra-site View and Individual View. First view shows an overview of the latest status in multiple first-aid stations. Second view shows detailed status of each first-aid station. Third view shows vital information of patients using the augmented reality technique[17]. Digital Right Management based on JPEG lossy compression describe the fundamental idea of DRM is to use incomplete cryptography and user identification mechanisms to control the quality of digital contents. Here prototyped JPEG codec control the open level of contents. At decoding process, an identification code embedded within authorized key prevent unauthorized duplication or business of digital data[18]. Importance of security and privacy in pervasive technology lead to the development of trustworthy pervasive video surveillance systems, by emphasizing the need to properly combine different aspects that current systems do not manage. In particular the combination of the following issues into a common framework: proper people identification mainly based on computer vision techniques, content protection not only by using convenient cryptography techniques, but also law enforcement and user co-operation in order to get feedback with regard to whole video surveillance system. Furthermore, an analysis focused on current computer vision technique used for people identification is presented. Finally, a score to measure trust offered by video surveillance system is included [19]. Using cryptographic identification protocol fragmented face can be reconstructed and the consequence of malformed input attack on the system. The study from security and computer vision standpoint reveals two aspects. Firstly, a attack that makes a dishonest user to undetectably extract a coded representation of faces on the list, and secondly, a visualization approach that turns the lossy recovered codes into human-identification face sketches. When evaluating face identification tasks thro' a compter and human subjects this approach underscores the major risk posed by malicious adversaries[20].

**5.CONCLUSION**

From its inception in 1994 visual cryptography remains an important topic for research. It is hoped that this paper will encourage more wide spread use of visual cryptographic techniques which can decode concealed images without any cryptographic computation. This is an added advantage of visual cryptography over other popular conditionally secure cryptography scheme and that more research in this area will be forth coming.

One area that future research should focus on is application of vc in medical environment with more concentration given to image quality and clarity which may serve to identify inherent complexity. This would be a great boon to cryptographic researchers in providing a better understanding of the force which moves the visual cryptography. Further a classification block-diagram is presented below over viewing the cryptographic survey. Figure 2 illustrates three aspects. First, it makes a broad classification, then it refines the classification by beginning more specific and its integrated into application environment.

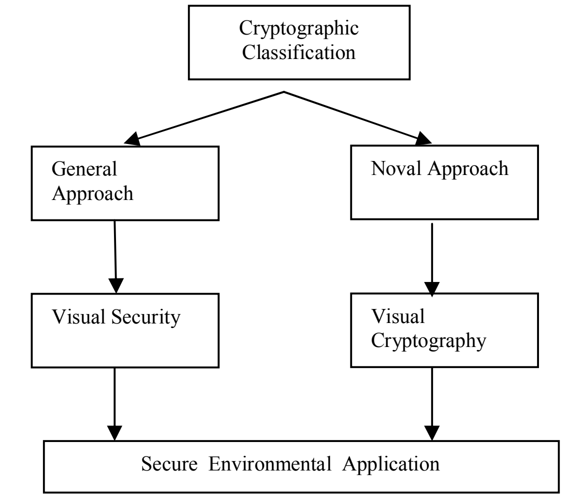


Figure2: Cryptographic Classification Block Diagram.

Finally Tabel. I shows the comparison between visual cryptography and other security mechanism, illustrating where these two differ.

| Scheme | Objective | Security measures | VC | Human decoding |
|---|---|---|---|---|
| Xiaoqing Tan[8] | Verify cheaters | Watermark extraction | yes | Yes |
| Kunal Sain[9] | Authentication & cheater detection | k-out-of-n VC | Yes | yes |
| Sascha Fahi[1] | Confidentiality & integrity | Symmetric encryption | no | no |
| Christopher Thorpe[16] | Improve data security | Spatial encryption | no | no |

Table I: Comparison between VC and other security mechanism,

## 6.REFERENCES

[1] Sascha Fahi, Marian Marian Harbach, Thomas Muders, Matthew Smith, "Confidentiality as a Service-Usable Security for the Cloud", trustcom, pp.153-162, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, 2012.

[2] Vipin Kumar, Chirag Chetan, Aparajita Ojna, "On a Visual Secret Sharing Scheme with High Quality Decryption", trustcom, pp.1200-1203, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communication, 2012.

[3] Alessandro Colantonio, Roberto Di Pietro, Albert Ocello, Nino Vincenzo Verde, "Visual Role Mining: A Picture Is Worth a Thousand Roles", IEEE Transactiona on Knowledge and Data Engineering, vol.24, no. 6, pp. 1120-1133, June 2012.

[4] Piergiuseppe Bettassa Copet, A. Pironti, D. Pozza, R. Sisto, P. Vivoli, "Visual Model-Driven Design, Verification and Implementation of Security Protocols," hase, pp. 62-65, 2012 IEEE 14th International Symposium on High-Assurance Systems Engineering, 2012.

[5] Marek R. Ogiela, Lidia Ogiela, "Medical Visualizations in Secure Bio Computing", waina, pp. 977-980, 2012 26th International Conference on Advanced Information Networking and Applications Workshops, 2012.

[6] Evgenia Novikova, Igor Kotenko, "Analytical Visualization Techniques for Security Information and Event Management", pdp, pp. 519-525, 2013 21st Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, 2013.

[7] M.Giordane, G.Polese, "Visual Computer-Managed Security: A Framework for Developing Access Control in Enterprise Applications", IEEE Software, vol. 30, no. 5, pp. 62-69, Sept-Oct, 2013.

[8] Xiaoqing Tan, Qiong Zhang, "A Kind of Verifiable Visual Cryptography Scheme", eidtw, pp. 215-219, 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2013.

[9] Kunal Sain, Mradula Sharmce, Suneeta Agarwal, "(Student Contribution) ASPS: an Authentication Scheme Using Pre-Formed Visual Cryptographic Shares", pp. 183-187, Proceedings of Fifth International Conference on Security of Information and Networks (SIN' 12), 2012.

[10] Yuanfeng Liu, Zhongmin Wang, "Halftone Visual Cryptography with Color Shares", grc, pp. 746-749, 2012 IEEE International Conference on Granular Computing, 2012.

[11] Xiao-Yi Liu, Ring-Song Chen, Ya-Li Zhang, "A New Color Visual Cryptography Scheme with Perfect Contrast", pp. 449-454, 2013 8th International Conference on Communications and Networking in China (CHINACOM), 2013.

[12] Hui-Wen Liao, "A Multiple Watermarking Scheme for Color Images", pp. 132-137, MUSIC. 2012. 30.

[13] Jonathan Weir, Mohan S. Kankanhalli, Weiqi Yan, "Image Hatching for Visual Cryptography", pp. 1-15, ACM Transaction on Multimedia Computing, Communications and Applications (TOMCCAP),2012.

[14] Shih-Fu Chang, Hyunjin Chung, Tai-Hsu Lin, Tao Cheng, Xianglong Liu, Jinyuan Feng, Junfeng He, "Mobile Product Search with Bag of Hash Bits and Boundary ReRanking", cvpr, pp. 3005-3012, 2012 IEEE Conference on Computer Vision and Pattern Recongnition (CVPR), 2012.

[15] Ahmetovic Dragan, "Independent Way-finding for visually Impared users through Multi-Sensorial Data Analysis on Mobile Devices", percomw, pp. 538-539, 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 2012.

[16] Christopher Thorpe, Feng Li, Zijia Li, Zhan Yu, David Saunders, Jingyi Yu, "A Coprime Blur Scheme for Data Security in Video Surveillance", IEEE Transaction on Pattern Analysis, and Machine Intelligence, vol. 35, no. 12, pp. 3066-3072, Dec. 2013.

[17] Teruhiro Mizumoto, Shinga Imazu, Weihua Sun, Naoki Shibata, Keiichi Yasumoto, "Emergency Medical

Support System for Visualizing Locations and Vital Signs of Patients in Mass Casualty Incident", percomw, pp. 740-745, 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 2012.

[18] Munetoshi Iwakiri, Ta Minh Thanh, "Fundamental InComplete Cryptography Method to Digital Rights Management Based on JPEG Lossy Compression", aina, pp. 755-762, 2012 IEEE 26th International Conference on Advanced Information Networking and Applications, 2012.

[19] Antoni Martinez-Balleste, Hatern A. Rashwan, Domenec Pulg, Antonia Paniza Fullana, "Towards a Trustworthy Privacy in Pervasive Video Surveillance Systems", percomw, pp. 914-919, 2012 IEEE International Conference on Pervasive Computing and Communications Workshops.

[20] Andy Luong, Michael Gerbush, Brent Waters, Kristen Gravman, "Reconstructing a Fragmented Face from a Cryptographic identification Protocol", wacv, pp. 238-245, 2013 IEEE Workshop on Applications of Computer Vision (wacv), 2013.