Securing Cloud Data and Cheque Truncation System with Visual Cryptography

Jaya
Symantec Software India Pvt. Ltd.
Pune - 411014
Maharashtra, India

ABSTRACT
Cloud computing is growing day-by-day in the current world scenario. Organizations are excited and worried at the same time to use cloud computing features as it will require for them to move their data on public cloud. Resource utilization is the main advantage of cloud computing which results in storing data of multiple clients in one place. Private cloud is preferred by the companies but it does not provide all the advantages of cloud computing. Cloud providers are working hard to secure their infrastructure and the stored data in cloud. To secure data, encryption is the most preferred solution. But the problem with traditional cryptographic methods is that they take huge amount of computation power and time in processing the encrypted data. Visual Cryptography is a cryptographic method which takes less amount of time to encrypt or decrypt data and can be applied in the field of cloud to improve its security parameters. It can also be used in the financial field such as Cheque Truncation System to transfer the images securely.

General Terms
Security, Cryptography, Steganography et. al.

Keywords
Cloud computing; visual cryptography schemes (VCS); share; pixel expansion; stacking.

1. INTRODUCTION
With network growing rapidly, there is an urgent need to ensure information security in the present era of electronic commerce. Internet has become the primary source of transmitting confidential data such as military information, financial documents, etc. Currently many security providing tools are used to make the communication reliable over network. Cryptography is one of the tools. It is not just a set of encryption-decryption algorithms but also applies to message integrity and authentication. The disadvantage of conventional cryptographic methods is that they need a lot of time and computation power for performing encryption and decryption. In addition to that, these methods are susceptible to many security attacks. So, some new scheme should be looked forward to, which can provide confidentiality with simpler techniques. In 1994, Naor and Shamir [1] proposed a new cryptographic area called visual cryptography based on the concept of secret-sharing. It divides an image into a certain number of shares and requires threshold number of shares to retrieve the original image. The decrypted message is obtained from stacking of the shares. The most notable characteristic of this scheme is to have a computation-less decryption. One of the extensions of the basic scheme is that it can also be used for applications which do not want to trust every participating entity in the process, using General Access Structure scheme. Another interesting extension of the original model is to generate innocent-looking shares so that attacker cannot get doubtful by looking at the random pattern of the share. Visual Cryptography is expanded to encode multiple secret images together so that overhead of generating and keeping too many shares can be reduced. [2], [3], [4], [5] and [6] discuss such techniques of multiple secret sharing. One other advancement in this field has been done to encode multi-pixels at once in order to reduce the share size and make the performance better. Few of the methods are discussed in [7] and [8].

The NIST definition of cloud computing [9] says that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Computing and storage are delivered as a service to the users. Cloud computing is one of the most significant shifts in information technology. It is getting popular day-by-day. But at the same time, there are many security and privacy issues related to cloud computing. Few of the threats are identified by CSA [10]. The biggest concern is that organizations lose control over their data which is stored in cloud. In this paper, visual cryptography has been used as a tool to reduce effects of few of the cloud security threats.

Cheque Truncation System (CTS) is an online image-based cheque clearing system, a project initiated by Reserve Bank of India for faster clearing of cheques. In this, scanned image of cheque is sent electronically to remove the need of manual/physical transfer of cheques. Visual cryptography is a perfect tool to secure the images and it can be applied effectively here.

The paper is organized as follows: Section 2 presents the basic scheme of Visual Cryptography, proposed by Naor and Shamir [1]. Section 3 describes the top threats to cloud computing, identified by CSA. Section 4 proposes few methods to improve security and privacy for cloud using visual cryptography. Section 5 contains the experimental results for verification of the proposed schemes. Section 6 presents the application of visual cryptography to secure Cheque Truncation System.

2. RELATED WORK

2.1 (2,2) Visual Cryptography Scheme
A (2,2)-VCS scheme divides the original image into 2 shares and secret image is recreated by stacking both the shares one over the other. Secret image is viewed as a collection of white

and black pixels. Each share contains collections of m black and white subpixels where each collection represents a particular original pixel. The resulting picture can be thought as a [n x m] Boolean matrix S = [si,j].

si,j = 1 if the j-th subpixel in the i-th share is black.

si,j = 0 if the j-th subpixel in the i-th share is white.

The algorithm, in Figure 1, describes how to encode a single pixel. One of the two subpixels in P is black and the other is white in both the shares. The possibilities "black-white" and "white-black" are equally likely, independent of the corresponding pixel in the secret image. So the shares do not provide any information as whether the original pixel to be encoded is black or white and hence proves the security of the scheme.

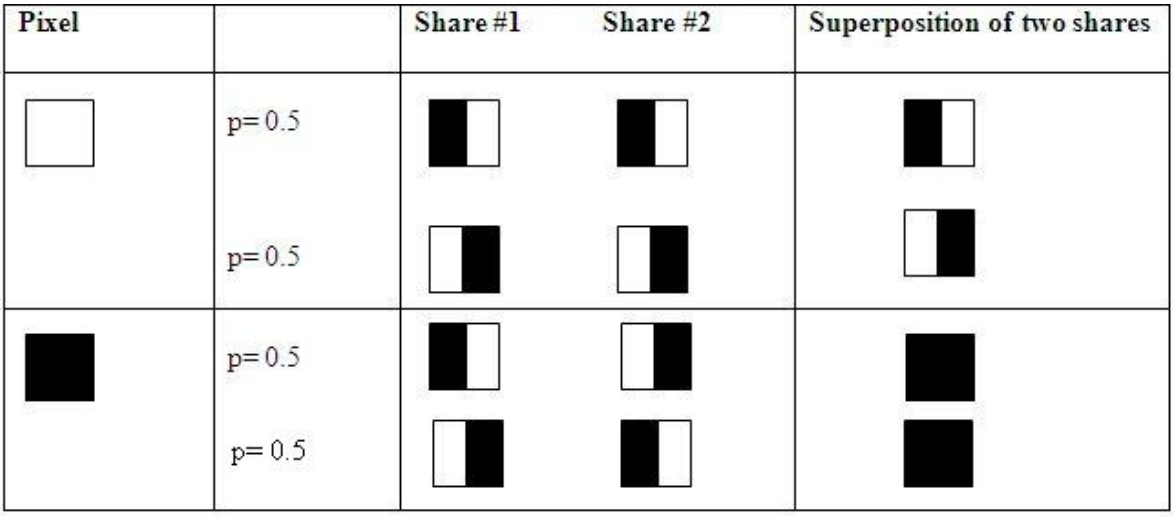


Fig 1: Encoding and stacking of a single pixel

3. THREATS TO CLOUD COMPUTING

3.1 Abuse and Nefarious Use of Cloud Computing

Companies and individuals are hesitant in using cloud computing. One of the reasons is that people are not trained to use this technology. Some cloud service providers are offering free limited trial periods to give people a feel of cloud computing. But it has weak registration protocols and authentication systems that allow anonymity. This is leading to several attacks targeted on IaaS and PaaS such as, password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables and CAPTCHA solving farms. [11] and [12] show such type of attack information on Amazon EC2.

3.2 Insecure Application Programming Interfaces

Many cloud computing vendors provide APIs or interfaces which is to be used by customers to interact with cloud services. Using these APIs cloud vendors do provisioning, management, orchestration and monitoring. Attackers often try to find security loopholes in the interfaces to manipulate authentication and access control over the resources. A weak set of interfaces and APIs arise security issues related to confidentiality, integrity, availability and accountability. API vulnerability can lead to many attacks, which is discussed in [13]. The recent example is LinkedIn attack [14].

3.3 Malicious Insiders

Organizations are concerned about the IT security threats posed by outsiders. Countermeasures such as firewalls, antivirus software, and intrusion detection systems are enforced against these threats. Yet most significant damage to the organizations is done by malicious insiders. The access level granted to such an adversary can lead to fraud, loss or theft of confidential information. The threat caused by malicious insiders is discussed in [15].

3.4 Shared Technology Vulnerability

One of the goals of cloud computing is resource sharing. IaaS vendors deliver their services in a scalable way by sharing infrastructure. Disk partitions, shared servers, CPU caches, etc., are all shared between multiple clients. At the same time, cloud providers must ensure that customers do not have access to cloud's other tenant's actual or residual data, network traffic, etc.

3.5 Data Loss/Leakage

There are many ways to lose data. It can be deleted or altered during some operation without taking a backup. Loosing the encoding key for encrypted information results in having garbage data. Insufficient AAA (authentication, authorization, and audit) control can also lead to data loss or leakage. Few other examples are storage on unreliable media, data centre reliability, natural disaster, etc.

3.6 Account, Service

There are many ways to lose data. It can be deleted or altered during some operation without taking a backup. Losing the encoding key for encrypted information results in having garbage data. Insufficient AAA (authentication, authorization, and audit) control can also lead to data loss or leakage. Few other examples are storage on unreliable media, data centre reliability, natural disaster, etc.

4. THE PROPOSED SCHEME

Visual cryptography can be applied to secure cloud in following areas:

1. Meaningful share creation for data in-transit
2. Predicate encryption for minimal decryption of data

3. RBD (Role Based Decryption) for access control

4.1 Meaningful Share Creation for Data-in-transit

Meaningful share technique of visual cryptography can be used to hide data in-transit in cloud computing. In [6], authors have proposed a method to hide secret images with meaningful shares. These shares look like innocent images and do not attract attacker's attention. This method can also be used to hide multiple images together, so that space required to store the shares and overhead of share management can be reduced. The scheme takes two copies of single cover image for producing two innocent-looking shares of the secret image. When these two shares are XORed as part of the decryption process, the original embedded information can be achieved. Multiple secrets can be shared together with enhanced security. The advantages of the proposed method are good image quality, no additional data structure and less encoding time. The size of reconstructed images does not vary with the number of colors present in the secret images.

4.2 Predicate Encryption for Minimal Decryption of Data

Predicate encryption is a form of asymmetric encryption where different individuals (or groups) can selectively decrypt encrypted data instead of decrypting all of it. Predicate encryption is a way that can help limit decryption of huge amount of data for processing in cloud. Visual cryptography can be used to implement predicate encryption for secret data stored in cloud. The scheme described below, explains application of predicate encryption with visual cryptography.

Let us take a secret image A. Suppose it has shares as S1 and S2. This secret is shared between 4 users. But all the users do not need to know full secret. Suppose user 1 has access privileges to know secret A1, user 2 as A2, user 3 as A3 and user 4 as A4. Shares 1 and 2 can be formed such that after decryption, user 1 will be able to see only portion A1 and so on. This way, there will be one common share as S1. With the metadata of share S2, the access right of a user can be stored as which users are allowed to see which portion. Suppose user 1 is trying to view the secret. At the time of processing, portion A1 of S2 will be left as it is and other portions (A2, A3, A4) can be masked. This way, user 1 will only see A1 and rest of the secret will be blank and hidden.

4.3 RBD (Role Based Decryption) for Access Control

Role based decryption can be used to provide access control over the data stored in cloud. It can provide protection against unauthorized access and data loss. Here role based decryption means that data will be encrypted in the same way for all the users. But the decryption will be based on the role of the user. It can be understood in following method.

Let us take a secret image A. Suppose it has shares as S1 and S2. This secret is shared between 4 groups. But not all the groups are authorized to know full secret. Suppose group 1 has access privileges to know secret (A1), group 2 as (A1, A2), group 3 as (A1, A2, A3) and group 4 as (A1, A2, A3, A4). Shares 1 and 2 can be formed such that after decryption, group 1 will be able to see only portion A1 and so on. This way, there will be 1 common share as S1. With the metadata of S2, the access privilege of different groups can be stored. Suppose group 2 is trying to view the secret. At the time of processing, portion (A1, A2) of S2 will be left as it is and other portions (A3, A4) can be masked. This way, group 2 will only see (A1, A2) and rest of the secret will be blank and hidden.

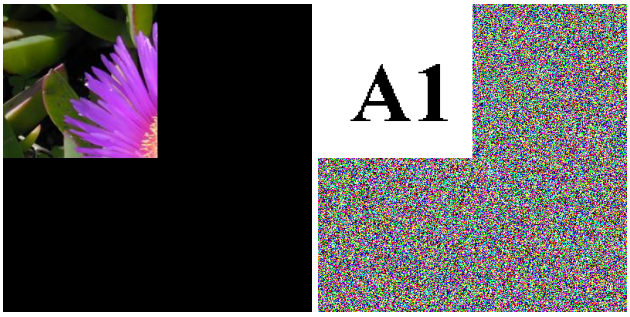
5. RESULTS

In this section, the results for applying predicate encryption and role based encryption with visual cryptography are presented. Pixel expansion used to produce the share of secret image is 4. The algorithm used to produce meaningful share is discussed in [6]. Figure 2(a) and 3(a) is the secret share. Figure 2(b) and 3(b) is the cover image. Cover image is used to hide the shares of secret image. Shares are created from the secret image and then embedded into the cover image. Same cover image has been used to hide the shares. It means that 2 copies of the same cover image are created. Copy 1 is used to embed share 1 and copy 2 is used to embed share 2. Figure 2(c) and 3(c) is the meaningful share 1 (share 1 of secret image which is embedded in cover image) and Figure 2(d) and 3(d) is the meaningful share 2 (share 2 embedded in cover image). The meaningful shares look like the original cover image and so serve the purpose of not attracting the attacker's attention.

5.1 Predicate Encryption

Figure 2(a) shows the secret image and 2(b) shows the cover image. Meaningful shares 2(c) and 2(d) are generated and stored already on the cloud server. Suppose user 1 is logged in and wants to see the secret image. Meaningful shares 2(c) and 2(d) are taken for processing. With the metadata of secret image 2(a), it is stored that user 1 is allowed to see only portion A1. So while processing, other portions (A2, A3, A4) of the meaningful share 2 are masked (set the pixel value to color black). After masking, share 2 appears as 2(e). Share 1 is left as it is. When the share 1and masked share 2 i.e. 2(c) and 2(e) are processed, the decrypted image appears as 2(f).

(a) (b) (c) (d)

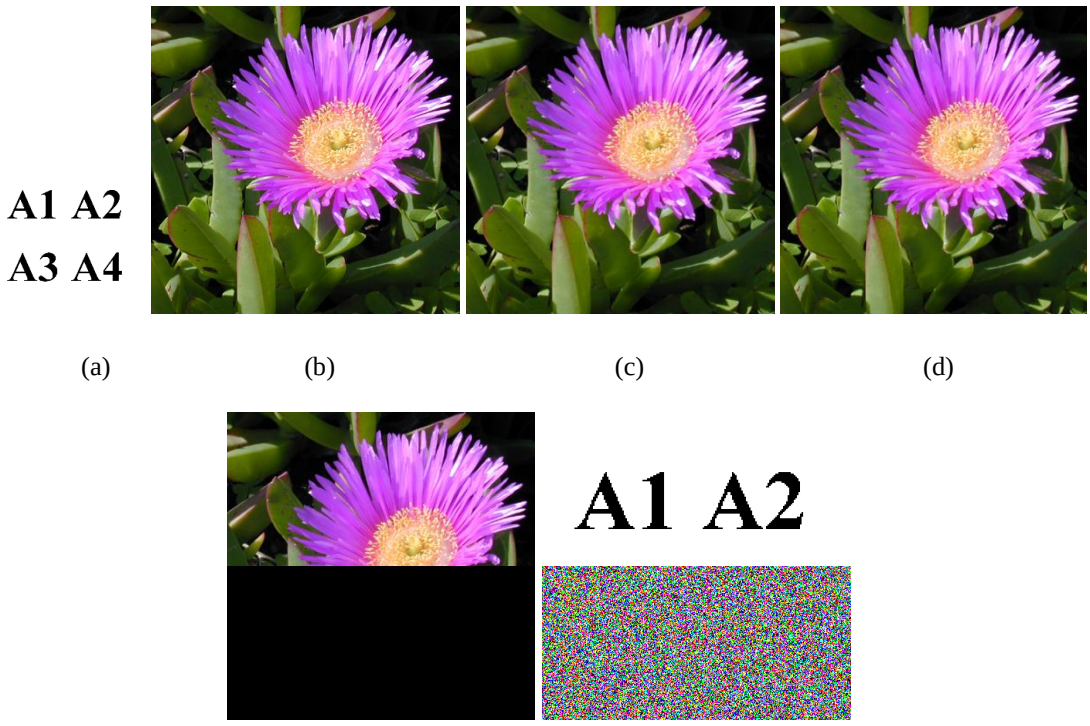


(e) (f)

Fig 2: Predicate encryption with Visual Cryptography
(a)Secret image (b)Cover image (c)Meaningful share 1 (d)Meaningful share 2 (e)Masked meaningful share 2 (f)Reconstructed image

5.2 RBD (Role Based Decryption)

Figure 3(a) shows the secret image and 3(b) shows the cover image. Meaningful shares 3(c) and 3(d) are generated and stored already on the cloud server. Suppose group 2 is logged in and wants to see the secret image. Share 3(c) and 3(d) are taken for processing. With the metadata of secret image 3(a), it is stored that group 2 is allowed to see portion (A1, A2). So while processing, other portions (A3, A4) of the meaningful share 2 are masked (set the pixel value to color black). After masking, share 2 appears as 3(e). Share 1 is left as it is. When the share 1and masked share 2 i.e. 3(c) and 3(e) are processed, the decrypted image appears as 3(f).



(a) (b) (c) (d)

(e) (f)

Fig 3: Role based decryption with Visual Cryptography
(a)Secret image (b)Cover image (c)Meaningful share 1 (d)Meaningful share 2 (e)Masked meaningful share 2 (f)Reconstructed image

6. CHEQUE TRUNCATION SYSTEM

Cheque Truncation System (CTS) is an online image-based cheque clearing system, a project undertaken by Reserve Bank of India for faster clearing of cheques [17]. Here the collecting bank branch would deploy scanned images along with the magnetic ink character (MICR) of the cheque which

will be sent out electronically using their Capture System, removing the need for physical/manual transfer of cheques. The captured images and the data is then signed, encrypted and sent to the Clearing House or the central processing location and thereafter forwarded to the drawee or paying bank. This helps speed up the cheque collection process that eventually helps provide better and faster customer service.

Visual cryptography is an effective tool to secure the cheque transaction system. In the system, scanned images are encrypted before transferring them electronically. This encryption can be done using visual cryptography. The scanned cheque image is divided into 2 share images. These share images are hidden in cover images [6] and sent separately to the drawee bank. Drawee bank then uses the secret shares hidden in cover images to get the original secret image. In addition to it, VC can also be used so that user can track status of the cheque clearing procedure. A receipt is created for the cheque by collecting branch (containing information such as amount, name of payee, etc.). 3 shares are created for this and original receipt can be reconstructed using (2,3)-threshold method. One share is kept by the collecting branch, another share is given to the user and third share is given to the drawee branch after cheque's shares are transferred. User can submit his/her share on collecting/drawee bank's site to know the status of cheque. Along with status, reconstructed receipt is also shown to verify the details. If the user finds any discrepancy, he/she can request the bank to stop the procedure. Same is the case with drawee bank. When the drawee bank receives cheques's shares and receipt's share, it checks with the collecting bank by submitting its receipt's share to get the cheque details. It verifies those details by reconstructing cheque's copy with cheque's shares hidden in cover image. If it finds anything suspicious, procedure is stopped/reinitiated. Figure 4 shows the flowchart for securing CTS.

This method has several advantages. First, if the user is not able to view reconstructed receipt or finds some discrepancy in it, can stop the transaction immediately by contacting collecting bank. Secondly, user can be ensured that no one can decode the receipt unless that person knows somehow the decryption algorithm and obtained atleast 2 secret keys held by collecting bank, drawee bank and the user. Finally, even if the both the meaningful shares are altered before reaching drawee bank, those details will not match with the details of reconstructed receipt and the drawee bank will stop the transaction in that case.

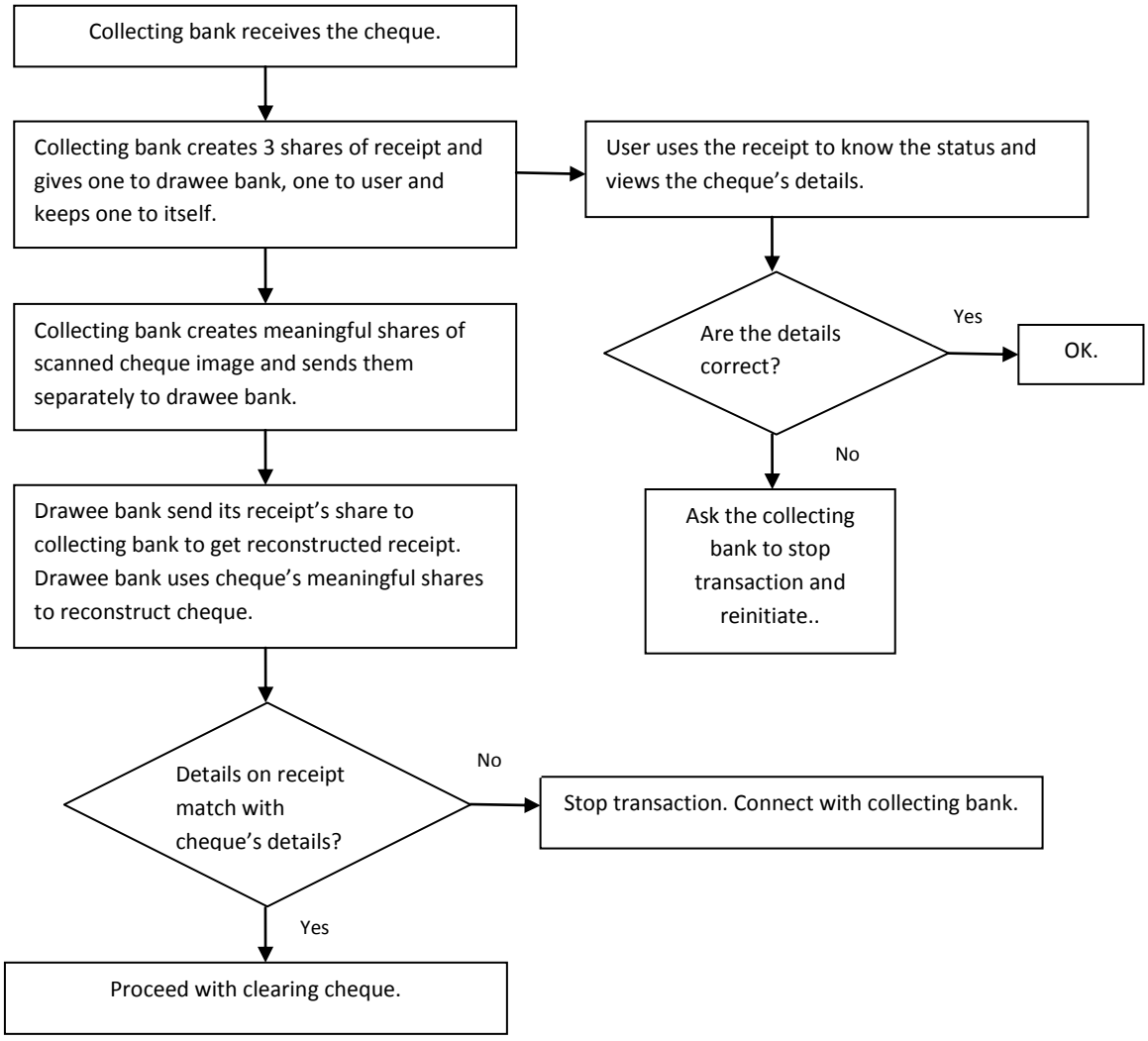


Fig 4: Flowchart for securing Cheque Truncation System

7. CONCLUSIONS

In this paper, visual cryptography is used to provide few methods to improve security and privacy of cloud. Visual Cryptography is an efficient technique which can be used to reduce probability of many threats to cloud. It can be used effectively in the areas of authentication, access control and encryption of stored data. Additional advantage of using VC is that it takes very less computation time than other traditional cryptographic methods. An application of VC is also presented to secure the Cheque Truncation System where the scanned cheque image needs to be protected. The field of visual cryptography is still evolving and it can be used as an important security providing technique in financial domain and for multiple areas of cloud computing.

8. REFERENCES

[1] Naor, M. and Shamir, A., "Visual cryptography", EUROCRYPT, LNCS, vol. 950. Springer, Heidelberg (1995), 1-12.

[2] Droste, S., "New results on visual cryptography", CRYPTO, LNCS, vol. 1109, Springer, Heidelberg (1996), 401-415.

[3] Wu, H.-C. and Chang, C.-C., "Sharing visual multi-secrets using circle shares", Computer Standards & Interfaces 28 (2005), 123-135.

[4] Shyu, S.J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., Chen, K., "Sharing multiple secrets in visual cryptography", Pattern Recognition 40 (2007), 3633–3651.

[5] Feng, J.-B., Wu, H.-C., Tsai, C.-S., Chang, Y.-F., Chu, Y.-P., "Visual secret sharing for multiple secrets", Pattern Recognition 41 (2008), 3572–3581.

[6] Jaya and Sardana, A., "Multiple Secrets Sharing With Meaningful Shares", In: International Conference on Advances in Computing and Communications. Springer Heidelberg, Part IV, CCIS 193 (2011), 233-243.

[7] Hou, Y.C., Tu, S.-F., "A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method", Journal of Research and Practice in Information Technology, vol. 37, (2005), 179- 191.

[8] Zhang, H., Wang, X., Cao, W., Huang, Y., "Visual Cryptographic for General Access Structure by Multi-pixel Encoding with Variable Block Size", International Symposium on Knowledge Acqusition and Modeling (2008).

[9] csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[10] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[11] http://blogs.zdnet.com/security/?p=5110

[12] http://voices.washingtonpost.com/securityfix/2008/07/amazon_hey_spammers_get_off_my.html

[13] http://securitylabs.websense.com/content/Blogs/3402.aspx

[14] http://www.esecurityplanet.com/hackers/lessons-from-the-linkedin-password-attack.html

[15] http://www.bankinfosecurity.com/blogs.php?postID=140

[16] http://bits.blogs.nytimes.com/2012/08/01/dropbox-spam-attack-tied-to-stolen-employee-password/

[17] http://en.wikipedia.org/wiki/Cheque_truncation_system