ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

An Innovative Solution for Cloud Security through Quantitative Analysis of Various Visual Cryptography Schemes

R. Kalaichelvi, Dr. L. Arockiam
Research Scholar, Department of Computer Science, Karpagam University, Coimbatore, India
Associate Professor, St. Joseph's College, Tiruchirappalli, India

Abstract - Cloud computing is an emerging powerful technology. With the help of ubiquitous internet technology, cloud providers offer numerous services to many sectors such as industry, academia, medical and the government. With the advent of cloud computing usage, adoption of cloud storage has become very simple. At the same time, providing data security becomes very momentous. The biggest impediment to the cloud environment is the deficiency of trust, which has stopped the shift of the whole of IT systems onto the cloud. Encryption is the genuine solution to mitigate data security risks. But cloud service providers do not support encrypted data. Additionally, the conventional encryption techniques involve key management and other computational complexities. With better understanding of computational complexities and other scenarios, in this paper, visual cryptography is proposed to maintain data confidentiality. Additionally, a range of visual cryptography schemes are explored in terms of their unique properties.

***Index Terms*-Encryption, data security, visual cryptography, computational complexities, data confidentiality.**

I. INTRODUCTION

Cloud computing is an on demand computing in which dynamically scalable and often virtualized resources are provided as a service. It is a methodology that takes the help of the internet to provide services like storage for the end users, computations, database driven services for different sectors of industries such as financial, healthcare, education and the government. Cloud model utilizes the computing resources with the capabilities of expanding the resources, providing pay per user privilege with a little or no up-front investment costs on IT infrastructure. The cloud computing services are delivered through Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [4]. A cloud setup can be private or public cloud.

A. Data Security

Every day, the needs for computing resources are increasing. As data is growing at a rapid rate in enterprises, costs involved in storing and maintaining data is also increasing [3]. The de-facto solution in reduction of storage cost is outsourcing data to cloud computing [1]. Cloud computing establishes a new domain of opportunity for businesses, but the move to cloud computing brings in a number of aspects that require special consideration when it comes to securing data. The promising model, cloud computing moves applications and databases to the large data centers [2]. However, the management of the data and services [16] may not be fully trustworthy and the enterprises may not have any control on data, since the data centers are remotely located. The common security concerns are: 1.securing data in transit and at rest, 2.secure software interfaces, 3.user access control, and 4.Data separation. Since, data in cloud computing is placed in the hands of third parties, ensuring the data security both at rest (data residing on storage media) as well as when in transit is of greater importance. The user's data integrity and confidentiality are maintained by providing data security, which is an important quality of service in cloud computing.

B. Encryption

Security of data in cloud is a challenge and is of supreme importance as many flaws and concerns are yet to be identified. As data is stored in the cloud, the user does not know where it is stored and who all can access the data. Naturally, the data owners worry about the confidentiality and integrity of the data. To ensure data confidentiality and integrity, the data owner must provide security for their data before they store the data on cloud. Hence, a technique should be incorporated to have the data stored securely on cloud. The technique used for data protection is encryption. Data encryption provides security for data transmission and data storage. Various cryptographic algorithms are proposed which can make the world of cloud computing more secure, reliable and admirable in such a diminutive time. The Fig. 1 depicts the process of data security using encryption technique.

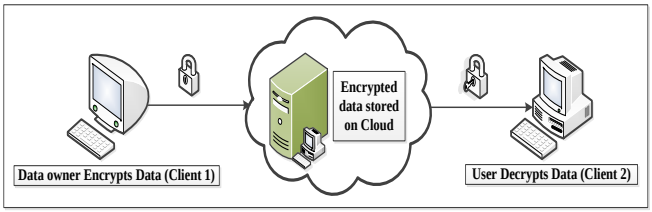

Fig. 1. Secured Cloud Storage

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

The processes of encoding and decoding are known as Cryptography. Cryptography encodes a plain text to a cipher text and decodes the cipher text to plain text. There are two types of cryptography algorithms namely symmetric algorithm and asymmetric algorithm. Symmetric algorithm uses a single secret key while asymmetric uses two different keys for encryption and decryption. In either case, a lot of computation and key management is involved. Moreover, user needs to have knowledge of cryptography.

C. Visual Cryptography

Visual Cryptography is a scheme with which any static media such as text or images can be encrypted in a secure manner. At the same time, the decryption does not need any cryptographic knowledge. Without any computation, the decryption can be done in a simple and secure way by human eyes. Visual cryptography (VC) was developed by Moni Naor and Adi Shamir at *EUROCRYPT 1994* [5]. The technique consists of two parts: 1. Cipher - The original text is encoded as cipher text 2. Secret Key - a transparency. The cipher text and the key on a transparency page reveal the original text. Secret Sharing Scheme: (n, n)-VCS [5] scheme was introduced by Naor and Shamir. In the (n, n)-VCS scheme n encoded shares of original image are printed on n transparencies. The superimposition of all n shares stacked on each other can be formed as the original image and can be simply recognized or visualized by human eyes without any cryptography computation. The first scheme was (2, 2)-VCS where 2 out of 2 secret shares are stacked together. Then (k, n)-VCS was investigated by Shyu and Chen [6]. In conventional (k out of n) - VCS, one secret image P is encoded into n shares and printed on n transparencies. To decrypt the original image, any k or more shares are superimposed together to have a human visual recognition. While less than k shares cannot obtain the secret image.

Traditional VCS encodes a secret image into n shares that persuades two conditions [7].

1. A qualified subset of shares
2. A forbidden subset of shares.

k and more than k shares which are used to reveal the secret image is known as qualified shares, while less than k shares which cannot reveal the information is known as forbidden shares.

There are two categories of decoding process to decrypt the original image.

1. Direct Stacking - the minimal number (k or more than k) of transparencies are superimposed together directly.
2. Additional supporting functions before stacking - additional operations such as flipping, rotation applied on one or more transparencies before superimposition.

II. BASIC MODEL

In the simplest version of the visual cryptography scheme, a secret image is divided into n number of shares. The idea of Visual Cryptography (VC) technique was first introduced by Naor and Shamir [5]. The Visual Cryptography Scheme is denoted as (k, n) VCS or k out of n secret scheme, where $k \leq n$. The secret is encoded on to n shares or transparencies. Decoding process involves human visual perception and superimposition of shares (transparencies). It does not require any computation or computation device. When any group of k or more than k shares are superimposed, it becomes human visual recognition image. Whilst when less than k shares are stacked, no information can be acquired. Let P, the image, be a set of black (1) and white (0) pixels. Here each pixel is divided into two sub-pixels, which are collection of black (11) and white (00) sub pixels. Further, the sub-pixels are divided into two sections with black and white (10) regions and white and black (01) regions. Fig. 2 shows the encryption process of sub pixels into black and white colors. These distributions of sub-pixels are referred to as the pixel expansion. The quality of a VCS depends on the pixel expansion and the contrast of the superimposed image.

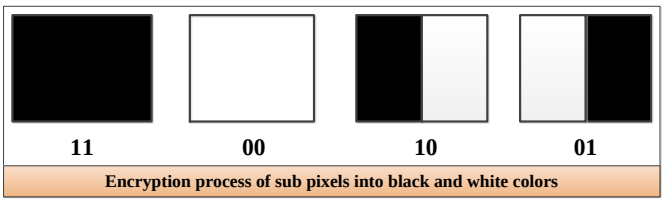

Fig. 2. Encryption process of sub pixels into black and white colors

By overlapping the k shares into stack, the original image P is revealed. The overlapping shares into stack is just like as a Boolean - OR (V) operation [10]. Fig. 3 shows the overlapping steps.

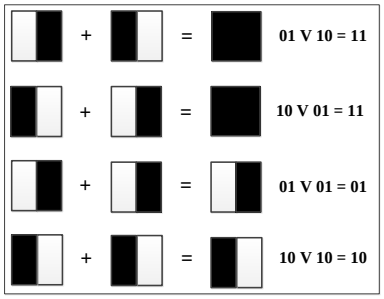

Fig. 3. Boolean OR operation [10]

III. VISUAL CRYPTOGRAPHY SCHEMES (VCSS)

A. Visual cryptography scheme with sharing of one secret image

Conventional Threshold Visual Secret Scheme [5], [8], [9] encodes one secret image S onto n transparencies. The transparencies are called shares. These n shares are dispensed to the n users. In decoding process, any set of k or more than k out of n shares are used to get the original

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

image, when they are stacked together. Whereas, when less than k shares are superimposed, then the S cannot be revealed. Threshold secret sharing scheme is denoted as (k, n) visual secret scheme or k out of n secret scheme, where k ≤ n or k, n threshold structure. Two significant factors which affect the quality of the reconstructed image are pixel expansion and contrast. The best possible pixel expansion of (k,n)-VCS is $m_{(n,n)} = 2^{n-1}$. The contrast is $1/2^{n-1}$. The Fig. 4 depicts the visual cryptography scheme with one secret image.

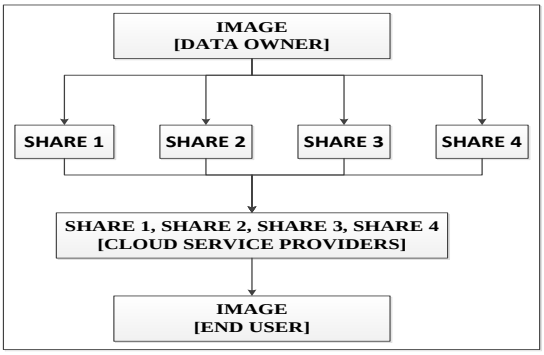

Fig. 4. Visual Cryptography Scheme with One Secret Image

Definition of Threshold VCS

Let n - be the number of shares; m – be the number of subpixels; C_0 – be the 23Collection of n x m matrices for transparencies of white pixel; C_1 - Collection of n x m matrices for transparencies of black pixel. The threshold VCS comprises of two nxm Boolean matrices with C_0 and C_1. C_0 and C_1 are called share matrices. One of the matrices in C_0 will be chosen to share a white pixel, while to share a black pixel, one of the matrices in C_1 will be chosen.

There are two criterions namely contrast criterions and security criterion are met to have a solution to (k, n)-VCS [5].

Contrast criterions: Guarantee the presence of the difference in the weight of the collective transparencies of black and white pixels. It helps the human's ability to make out the color of pixels. There are 2 conditions involved in contrast criterion of (k, n) - VCS.

1. $H(V) \leq d - \alpha m$
2. $H(V) \geq d$

Where, H(V) is the hamming weight; m is pixel expansion; α - relative difference or contrast of the revealed image; d-the threshold of a qualified subset.

***Security criterion*:** Ensures the information security on the color of pixels. i.e with lesser than k shares, no information can be obtained about the secret image.

Disadvantage of the traditional VCS is that they cannot deal with the gray-scale image. The following are the Visual cryptography scheme with sharing of one secret image.

1. Conventional Threshold Visual Secret Scheme - (k, n) VCS
2. VCS with extended capabilities where the shares may be meaningful
3. VCS with general access structures
4. Color VCS
5. Contrast of VCS
6. Pixel expansion of VCS.

B. Visual cryptography scheme with sharing of multiple secret images

In this scheme multiple (s) secret images are shared by n users referred to as Multiple Secret Visual Cryptography Scheme (MVCS). The Fig. 5 represents Multiple Secret Visual Cryptography Scheme.

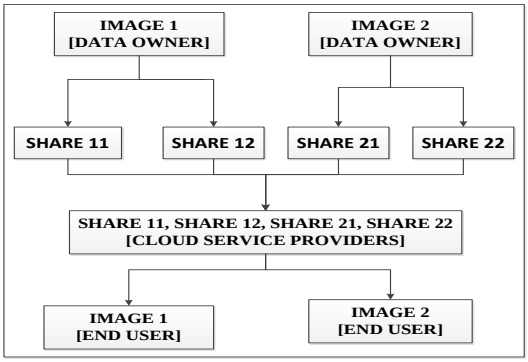

Fig. 5. Multiple Secret Visual Cryptography Scheme

There are two popular MVCSs namely (k, n, s)-MVCS [8] and (k, n, s, R)-MVCS [8].

1) (k, n, s) - MVCS:

In (k, n, s) - MVCS, s secret images P_1, P_2, ... P_s are divided into n transparencies S_1, S_2, ... S_n. These transparencies are disseminated to n users. First secret (P_1) is revealed by superimposition of k shares; Second secret (P_2) is revealed by superimposition of k+1 shares; and sth secret (P_s) is revealed by superimposition of n shares respectively.

Where,

s = number of secret images; s = n - k+1(≥2);

n = number of users or number of shares;

k = threshold value of shares to reconstruct the secret image.

2) (k, n, s, R)-MVCS

With s secret images P_1, P_2, ... P_s, a factor called revealing list R is involved in encoding process of (k, n, s, R)-MVCS.

Where,

R: revealing list= $\{r_k, r_{k+1}, ..., r_n\}$

$r_u \in \{0,1,2,.....s\}$ for $k \leq u \leq n$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

r_u = t if P_t is reconstructed or r_u = 0 if no secret is reconstructed.

and $1 \leq t \leq s$; $2 \leq s \leq n-k+1$..

C. Extended Visual Cryptography Scheme (EVCS)

An Extended Visual Cryptography Scheme (EVCS) [7] is like traditional VCS, but has meaningful transparencies. The EVCS is a more secured scheme than traditional VCS as it has meaningful images, the shares cannot be easily guessed. The following EVCSs are in use at present:

1. EVCS for natural images [11].
2. A simple EVCS where its shares are generated by replacing the white and black sub pixels in a traditional VCS. [12]
3. Halftoning techniques EVCS [13].
4. Error diffusion halftoning technique EVCS[14].

The limitations and disadvantages of EVCSs are:

1. Pixel expansion.
2. Bad visual quality of shares and the revealed secret images.
3. Computation expensive
4. Requirement of complementary images for revealing secret images.
5. Visual effect of shares affects other shares' content.

D. Half toning Technique or Dithering Technique

The traditional VCS works only with black and white image not with the gray-scale image. The halftoning technique is used to deal with the gray-scale image. The halftoning technique is also called as dithering technique. This technique converts the gray-scale image into binary image. After the conversion the traditional VCS is applied to encode the secret image. Patterning dithering algorithm is one of the techniques to convert the gray-scale image into binary image [13].

E. Visual Cryptography scheme for Color images

In general, the basic color models are the additive color model and the subtractive color model. In additive approach, red, green and blue are the primary colors. By mixing these primary colors, we get the secondary colors. In the subtractive approach CMYK color model is being used. By mixing Cyan, Magenta and Yellow, a wide range of colors can be produced. By subtracting one of the primary colors (Red, Green and Blue colors) from white we get any one of C, M & Y colors.

In VCS for color images technique [15], a color secret image is split into four halftone images namely cyan image, magenta image, yellow image and black image in a disorder manner. The black mask is used to hide the expected colors in the stacked image. These black pixels would not meddle with the momentous part of the image; rather it would be treated as image background. This technique expands each pixel into 2 x 2 block, 2 for color and 2 for transparent pixels.

IV. CONCLUSION

Cloud Computing is a boon to store a massive amount of data. The data in the cloud often ranges from public source, which has minimal security concerns to private data containing highly sensitive information. The biggest data security concern is that the owner may lose data as well as control of sensitive data since user data and business information resides in service provider's storage. This paper considers the problem of building a secure cloud storage using visual cryptography. In addition, we relate an overview of visual cryptography schemes from basic models to recent advanced schemes which can be integrated in cloud environment to provide trustworthy cloud storage.

REFERENCES

[1] D.H.Patil, et al., "Data Security over cloud", Emerging Trends in Computer Science and Information Technology -2012(ETCSIT2012), Proceedings published in International Journal of Computer Applications (IJCA), pp 11-14, 2012.

[2] Cong Wang et al., "Ensuring data storage security in Cloud Computing", Quality of Service, 2009. IWQoS. 17th International Workshop, Charleston, SC, pp 1- 9, July 2009.

[3] Sravan Kumar R et al., "Data Integrity proofs in cloud storage", Communication Systems and Networks (COMSNETS), IEEE, Bangalore, pp 1-4, 2011

[4] Seny Kamara et al., "Cryptographic Cloud Storage", Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization, Microsoft Research, p 1- 14, 2010

[5] M. Naor and A. Shamir, "Visual cryptography", In Proceedings of Advances in Cryptology--EUROCRYPT 94, LNCS, Vol. 950, Springer-Verlag pp. 1-12, 1995

[6] S. J. Shyu and M. C. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pt. 2, pp. 960–969, Sep. 2011

[7] Feng Liu et al., "Embedded Extended Visual Cryptography Schemes" , IEEE Trans. Inf. Forensics Security, Vol 6, No. 2, pp. 307 - 322, June 2011

[8] Shyong Jian et al., "General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes" IEEE Trans. Inf. Forensics Security, vol. 8, no. 5, pt. 2, pp.733–744, May 2013.

[9] G. R. Blakley, "Safeguarding cryptographic keys," in Proc. Nat. Computer, Conf., vol. 48, pp. 313–317 1979.

[10] Ankit Saxena, "Analysis of the various types of Visual Cryptography Schemes", Journal of Computing Technology, Vol 1, no. 4, pp 45 - 48, 2013

[11] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," in Proc. WSCG Conf. pp. 303–412, 2002.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

[12] D. S. Tsai, T. Chenc, and G. Horng, "On generating meaningful shares in visual secret sharing scheme," Imag. Sci. J., vol. 56, pp. 49–55, 2008.

[13] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography", IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[14] Z.M.Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[15] Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition, Elsevier, Vol 36, no. 7, pp 1619-1629, July 2003.

[16] Bhardwaj et al., "Cloud security assessment and identity management", Computer and Information Technology (ICCIT), 14th International Conference, Dhaka, pp 387-392, Dec 2011.

AUTHOR BIOGRAPHY

Engr. R. Kalaichelvi is working as an Asst. Professor in AMA International University, Kingdom of Bahrain. She is currently pursuing her research in Karpagam University, Coimbatore, India. She has published 7 research articles in the International / National Journals. Her areas of research interests are in Cloud Computing, Data Security, Cryptography and Data mining.

Dr. L. Arockiam is working as an Associate Professor in St.Joseph's College, India. He has published more than 140 research articles in the International / National Conferences and Journals. He has also authored two books: "Success through Soft Skills" and "Research in a Nutshell". He has presented two research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. His areas of research interests are: Software Measurement, Cloud Computing, and Cognitive Aspects in Programming, Web Service, Mobile Networks and Data mining. He has been awarded "Best Research Publications in Science" for 2010, 2011, & 2012 and ASDF Global Awards for "Best Academic Researcher" from ASDF, Pondicherry for the academic year 2012.