A Novel Approach onGenerating Secure Keys for Safety Locker using Extended Letter- Based Visual Cryptography

Dona Jose, M.Tech Student,
Department of Computer science
Government Engineering College Idukki,
Kerala, India

***Abstract*--In this era of technical innovations, numerous types of safetylockers are used. Most of the safety lockers use a single key throughout its usage. Hence the chances for security threats are higher. Security locks with more than a single key such as number lock are costly as well as vulnerable to threats since the key can be shared with unauthenticated persons or duplicated without being caught.**

The scheme for generation and sharing securekeys for security lockeris implemented using extended letter based visual cryptography. It is an extension of visual cryptographywhich is less computationally complex compared with traditional cryptographic schemes.The binary image of a key is divided into number ofkey shares. Any key share can be set as the locker's base key so that other key shares are used as key for that locker. Complete randomness is implemented in the generation of key shares to provide security. Each time the locker is locked, required number of new key shares is generated.

***Keywords-Key Share; Visual Cryptography (VC); Extended Letter based Visual Cryptography*.**

I. INTRODUCTION

Providing securityis a major task to attain in all the fields of technology. Along with the advancements in technology, security issues are also multiplied. Security locker is one of the widely used methods for the security of valuables. The security provided is mostly depends on the strength of the key used. The types of key, Difficulty of duplication, time period of usage of the same key are the major factors for strength of the key.

Traditional locker has a pair of keys which is unique for a locker and unalterable. Such keys can be duplicated with the help on a person who has access to the key. Since key is not missing, user may not be aware about the security threat. At a later time, the duplicate key can be used to open the lock because the key cannot be changed for such lockers. In some of the latest models of locker, biometric details are used for security. Even though it provide authentication of the user, sharing key will be difficult. Security locker with changeable number lock is one of the widely accepted schemes. It also has security issues like guessing attack, sharing key to unauthorized person etc. Hence it is not possible to find how many people know the key.

A new scheme based on extended letter based visual cryptography can be used in security lockers to provide better security and user acceptance. Every time the locker is locked, user can decide the number of keyshares to be generated. User can also fix the number of key shares needed to open the locker. One of the generated key shares is set as locker's base key. By inserting sufficient number of key shares to the locker can be opened.Extended Letter based visual cryptography is evolved from the visual cryptography proposed by Moni,Noar and Adi Shamir [1].

II.SECRET SHARING

A secret sharing scheme is a method for sharing a secret among a set *p* of *p* participants. The secret is encoded into *n* pieces called shares each of which is given to a distinct participant. There are two types of secret sharing scheme which are (*n*,*n*) secret sharing scheme and (*n*,*k*) secret sharing scheme.

A. *(n,n) Secret Sharing Scheme*

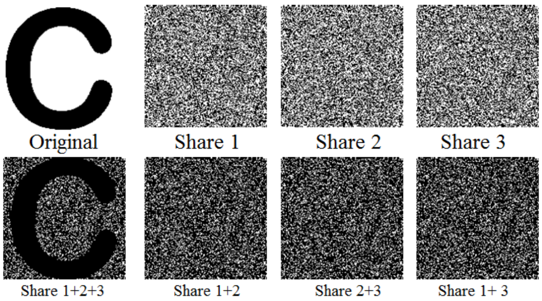

Fig 1: (3,3) Secret Sharing Scheme

In (*n*,*n*) Secret Sharing Scheme, *n* shares are generated. Out of the *n* generated shares, *n* shares are required to reveal the secret information. Retrieval of the information is impossible in (*n*,*n*) secret sharing when one of the shares is lost. In a (3,3) sharing scheme, all the 3 shares are needed to get the information

B. (*n*,*k*) Secret Sharing Scheme

In (*n*,*k*) Secret Sharing Scheme, all the n shares are not needed to reveal the information. It requires any of the k shares from the n shares. In a (3,2) sharing scheme, any two shares are needed to get the information.

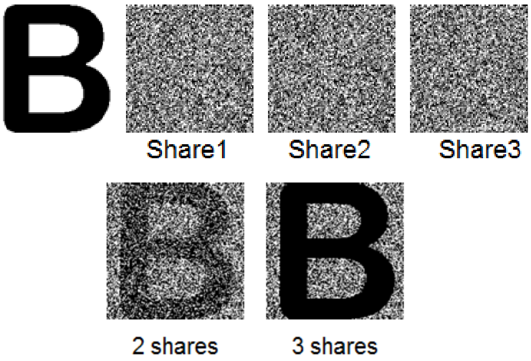

Fig 2: (3,2) Secret Sharing Scheme

III.VISUAL CRYPTOGRAPHY AND RELATED WORKS

Visual cryptography scheme is considered as a cryptographic technique which allows visual information to beencrypted, such a way that the decryption can be performed by the humanvisual system, without the aid of computers. There are various measureson which performance of visual cryptography scheme depends, such as pixelexpansion, contrast, security, accuracy, computational complexity, type of secret images and number of secret image encrypted by the scheme.

Visual cryptography scheme eliminates complex computation problem in decryption process, and the secretimages can be revealed by stacking operation. This property makes visualcryptography especially useful for the low computation load requirement.

Visual cryptography is divided into two categories based on the pixel expansion. They are Deterministic Visual Cryptographic Scheme (DVCS) and Probabilistic Visual Cryptographic Scheme (PVCS). In DVCS, the size of the secret image is expanded. It uses more than one pixel of share to represent a single pixel in the secret image. In PVCS, size of the secret image remains same. Either a black or white pixel is used to represent a pixel in the secret image.

Visual Cryptography has a wide range of research areas like colour visual cryptography, multiple secret visual cryptography, letter based visual cryptography etc.

Wu and Chen [2] proposed a scheme to hide two secret binary images into two random shares, namely A and B, in which the first secret can be seen by stacking the two shares, denoted by A XOR B, and the second secret can be obtained by first rotating share ‘A’ anti-clockwise. They designed the rotation angle θ to be 90. However, it is easy to obtain that θ can be 180 or 270.

To overcome the angle restriction of Wu and Chen’s scheme, Hsu et al. [3] proposed a scheme to hide two secret images in two rectangular share images with arbitrary rotating angles. Wu and Chang [4] also redefined the idea of Wu and Chen by encoding shares to be circles so that the restrictions to the rotating angles (θ= 90, 180 or 270) can be removed.

Until the year 1997 visual cryptography schemes were applied to only black and white images. First coloured visual cryptography scheme was developed by Verheul and Van Tilborg [5]. Colour visual cryptography is a potentially useful type of visual cryptography. It allows natural colour images to hide the information. Chang et al. present a scheme based on smaller shadow images which allows colour image reconstruction when any authorized *k* shadow images are stacked together. More shares are created for sharing purpose which reduces the overall size of the image.

Yang and Chen’s additive colour mixing scheme [6] allows for a fixed pixel expansion and improves on previous colour secret sharing scheme. But overall contrast is reduced when the secrets are revealed. In most of the colour visual cryptographic scheme, image gets darker when the secret recovered. It is due to the fact that image gets darker when two pixels of same colour are overlapped. In Cimato et al.’s scheme, it considers only three colours when superimposing. This allows for perfect reconstruction of a colour pixel, and no darkening occurs when pixels are superimposed or added.

Researches are also going on to improve the quality of the shares generated using the existing mechanisms. Recently ChingNung Yang and Yao-Yu Yang [7] proposed an extended visual sharing scheme to improve the shadow image quality. A meaningful shadow image is generated in the so-called extended visual secret sharing (EVSS) scheme.

In new EVSS scheme gray and white subpixels are used to represent the secret pixel. A digital halftoning technology is used in this method. When compared to the previous extended visual secret sharing scheme, ChingNung Yang and Yao-Yu Yang’s new scheme give clearer shadow images.

Fig 3: a) Secret Image

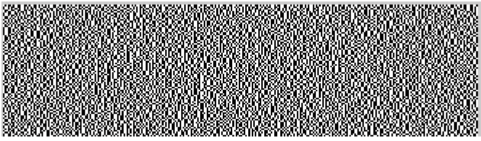

Fig 3: b) Share 1 using DVCS

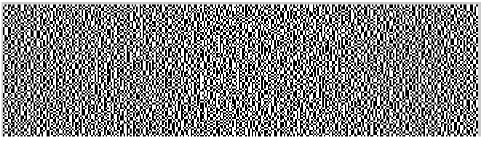

Fig 3: c) Share 2 using DVCS

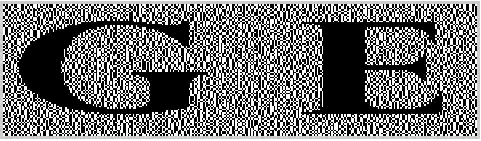

Fig 3: d) Overlapped shares using DVCS

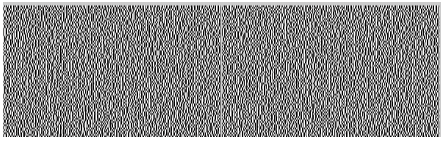

Fig 3: d) Share 1 and Share 2 using PVCS

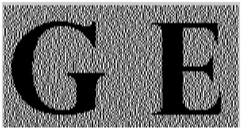

Fig 3: d) Overlapped shares using PVCS

IV. RELATED WORKS IN LETTER BASED VISUAL CRYPTOGRAPHY

Usual visual cryptographic scheme has noise-like shares which are unusual and suspected by censors when delivered by e-mail or fax. Also, noise-like shares are difficult to identify and manage when distributed. Letter Based Visual Cryptography replaces the noise like pixel representation with alphabets in any natural language. Use of morphological analyser improves natural appearance of the resulting shares by providing some meaningful sentences or words in shares

Takizawa and Yamamura [8] proposed two secret sharing schemes using natural language letters (Japanese). In the first scheme, the secret is revealed as the non-overlapped Japanese characters when stacking shares. All secret characters are placed in non-overlapped locations in each share, and the remaining space is overlapped by successive shares.

For the second scheme, the secret is revealed as a meaningful sentence in a particular column arising from the alignment of plain text sentences in a specific sequence. The authors employ a morphological analyser to carefully design their shares to try to prevent secret information leakage. However, Takizawa et al.'s two schemes cannot ensure Security.

The first method depends on the position of letters. Using their database and morphological analyser, secret messages complied by specific characters could be placed into specific positions and construct meaningful sentences in combination with other characters. Those secret message characters would not be overlapped when the shares are stacked. For reconstructing the secret messages, participators only stack enough shares and read the un-stacked characters.

Their second method also depends on the position of letters, but each share contains a secret letter. For the secret encoding phase, they separate the secret message into different shares with one character of the secret and compose a meaningful sentence using each secret letter with other words. For reconstructing the secret message, participators need to line up all the shares vertically in order, and the secret is revealed as a particular horizontal line. Their two methods both cover the secret in meaningful sentences, but their methods are not secure.

In 2013, Hsiao-Ching Lin and Ching-NungYang[9] introduced a scheme to overcome the drawbacks of previous schemes in letter based visual cryptography. It used overlapping of alphabets in shares to indicate the difference in contrast. Overlapping different alphabets result in a black pixel and overlapping same alphabets leads to white pixels. Adding more shares give better contrast. A return letter algorithm is used to select alphabets for the shares. Error tolerance is higher. Since the shares are meaningless, it is difficult to identify shares of a particular execution.

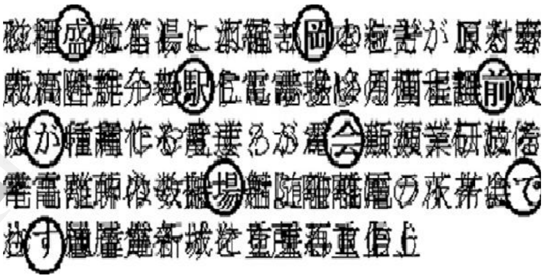

Fig4: Takizawa et al’s first scheme

V. GENERATION OF SECURE KEYS

Hsiao-Ching Lin and Ching-Nung Yang’s letter based visual cryptographic scheme along with some modifications is used for the generation of keys. DVCS is used for key generation.

A. *Pre-Processing*

A pre-processing stage is added before the share creation for better computational result.Binary key image can be selected randomly from a database of binary key images. It improves security. Even the main user of the locker will not be aware about the binary key image used to generate shares without merging the key shares.

In the pre-processing state, unnecessary parts of the binary key image is also discarded. It reduces the execution time. Storing all the possible combinations of alphabets can avoid the redundant analysis of possible combinations.

B. *Base Matrix Selection*

Based on the number of key shares to be generated and number of key shares needed to open the locker, some base matrices are used. The base matrices of (2,2) visual cryptographic scheme are B1 and B2.

Base matrices are the main element of key share creation. Base matrices are changed to change the scheme to have different number of keys. Base matrices are changed to corresponding letter matrices using return letter function.

$$B1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad B0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

C. Return Letter SelectionAnd Letter Matrix Generation

Letters for letter matrix generation is selected in random based on the pixel in the pre-processed binary image. A black pixel is represented with base matrix B0 and white pixel with base matrix B1. Letter matrix is generated from base matrix by replacing 0 with a letter which is already in that column. 1 is replaced by a different letter which is not present in that column. Each row in letter matrix indicates the corresponding pixel in particular share.

D. Key Share Generation

To generate the key shares, letter matrices are created for each pixel in the binary key image. Each row is placed in each share. So that, every pixel in the binary image is replaced with random letters.Complete randomness is implemented such that each execution has unique key shares. One key is selected as base key. In a (k,n) scheme, (n-1) key shares can be used by users and (k-1) key shares are required to unlock the locker. Since letter matrix varies on each generation, unique key shares can be generated. Previous key shares cannot be used to unlock the locker even though same basic key image is used.

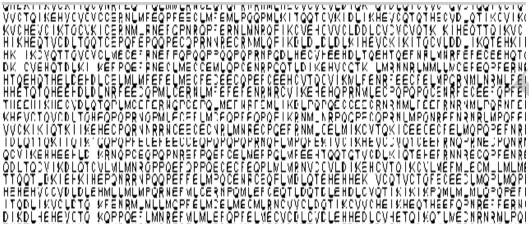

Fig 5: a) key share 1 in (2,2) scheme

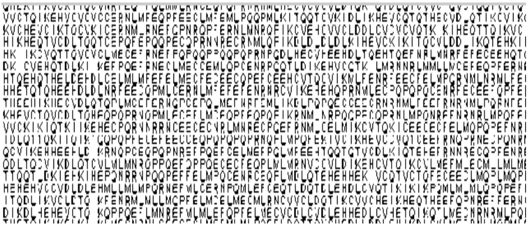

Fig 5: b) key share 2 in (2,2) scheme

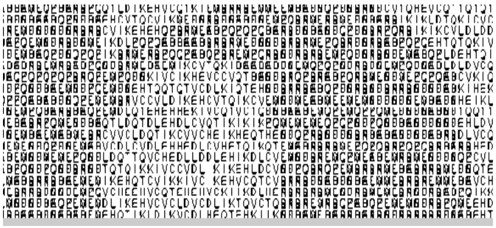

Fig 5: 3) Merged key shares to unlock (2,2) scheme

VI. CONCLUSION

Key share generation is implemented in Matlab(R2010a). Computational time is reduced compared with its previous schemes. With a hardware implementation, it can be implemented and safely used in security lockers.

VII. FUTURE WORKS

Authentication for key shares needed to be implemented. Some Mechanism is needed to identify key shares if multiple lockers are used by a user.

VIII. REFERENCES

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology,EUROCRYPT'94.Springer-Berlin-Heidelberg, 1995.

[2] C.C. Wu, L.H. Chen, “A Study On Visual Cryptography”, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[3] H.-C. Hsu, T.-S. Chen, Y.-H. Lin, “The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing”, in Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[4] Wu, Hsien-Chu, and Chin-Chen Chang. "Sharing visual multi-secrets using circle shares." *Computer Standards & Interfaces* 28, no. 1 (2005): 123-135.

[5] E. Verheul and H. V. Tilborg, ”Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes.” Designs, Codes and Cryptography,11(2),pp.179–196,1997.

[6] Yang, Ching-Nung, and Tse-Shih Chen. "Colored visual cryptography scheme based on additive color mixing." *Pattern Recognition* 41.10 (2008): 3114-3129.

[7] Yang, Ching-Nung, and Yao-Yu Yang. "New extended visual cryptography schemes with clearer shadow images." *Information Sciences* 271 (2014): 246-263.

[8] O. Takizawa, A. Yamamura, K. Makino, Secret sharing scheme using natural language text, Journal of the National Institute of Information and Communications Technology 52 (2005) 173–183.

[9] Lin, Hsiao-Ching, et al. "Natural language letter based visual cryptography scheme." Journal of Visual Communication and Image Representation 24.3 (2013): 318-331.