World Applied Sciences Journal 34 (4): 529-534, 2016
ISSN 1818-4952
© IDOSI Publications, 2016
DOI: 10.5829/idosi.wasj.2016.34.4.395

Keyed Visual Cryptography Scheme for Secure Data Transmission

Ch. Rupa and D. Sasidhar

Dept. of CSE, V. R. Siddhartha Engineering College (A), India

Abstract: A Visual Cryptography System (VCS) is a kind of secret sharing scheme. The rapid strides in technology have resulted in data being vulnerable to attacks. An attacker can easily identify the original image, if can they combine the shares of the original data image. In order to reduce these attacks we propose a new approach termed as Keyed Visual Cryptographic Scheme (KVCS). This would raise the computation factors which gives more security to the image data. In KVCS, each input share of the original image is encrypted with some shared key share using mathematical operator. Finally, the original image which should be shared covertly would be encoded into two shares and sent through the network. A person outside this sharing would not be able generate original image even by stacking the encrypted images. The main strength of this paper is cryptanalysis reports.

Key words: KVCS · VCS · Self Similarity · Shares · Encryption · Decryption

INTRODUCTION

Information technology plays a vital role in the current times. The rapid pace of technology had resulted in data in its various forms like text, image, audio or video is vulnerable to a host of attacks like hacking, unauthorized accessing etc. Information tracking, hacking and spoofing which are unethical have been done tried by unauthorized technocrats to transform data [1]. In view of this, information has been modified, updated and digitalized to circumvent this problem. Sometimes, these advances in the growth of the technology are prone to attacks by unauthorized people to alter the data, update the information while transmitting. Hence a novel cryptographic scheme was proposed - Visual Cryptographic scheme (VCS) without any cryptographic computation [2]. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model proposed herein is to split a secret image into two random shares (printed on transparencies) which individually reveal no information about the secret image other than that of the size of the secret image. Each component image has a pair of pixels for every pixel in the original image [3]. These pixel pairs are shaded black or white according to the following rule: if the original image pixel was black, the pixel pairs in the component images must be complementary; randomly shade one black and white, and the other white and black. When these complementary pairs are overlapped, they will appear dark gray. On the other hand, if the original image pixel was white, the pixel pairs in the component images must match: both black and white and both white and black. When these matching pairs are overlapped, they will appear light gray. So, when the two component images are superimposed, then only the original image appears. However, individually on its own a component image reveals no information about the original image; it is indistinguishable from a random pattern of black, white / white, black pairs. Moreover, if you have one component image, you can use the shading rules above to produce a counterfeit component image that combines with to produce no image at all.

The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions such as any qualified subset of shares can recover the secret image and second condition is any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image. Let S = {1,...,n} be a set of elements called participants, and let 2S denote the set of all subsets of S. Let us assume that the secret image consists of a collection of pixels, where each pixel is associated with a grey level

Corresponding Author: Dr. Ch. Rupa, Department of CSE, V.R. Siddhartha Engineering College (A), India.

ranging from white to black and each pixel is handled separately. Each pixel appears in ‘n’ versions called shares, one for each transparency [4]. Each share is a collection of ‘k’ black and white sub pixels. The resulting structure of the shares can be described by an n×k Boolean matrix T = [tij] where tij = 1 iff the jth sub pixel in the ith transparency is black. Therefore the grey level of the combined share, obtained by stacking the transparencies i1,...,is, is proportional to the Hamming weight w(V) of the mvector V = OR(ri1,...,ris), where ri1,...,ris are the rows of S associated with the transparencies we stack. Visual cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended recipient ever realize the original image, a form of security through obscurity [4,5]. By contrast, cryptography obscures the original image, but it does not conceal the fact that it is not the actual image. In this system we have a secret image which is encoded into N shares printed on transparencies. Any two of the shares are stacked on top of another and the secret image becomes decipherable to the human eye. After generating the covering shares, the embedding process can be realized by the following algorithm.

Algorithm 1. Embedding Process

Input: The corresponding VCS (d0, d1) with pixel expansion and the secret image.
Output: The n embedded shares x0,x1,....xn-1.
Step 1: Dividing the covering shares into blocks that contain (t = k) sub pixels each.
Step 2: Choose m embedding positions in each block in the n covering shares.
Step 3: For each black (respectively, white) pixel in I, randomly choose a share matrix K ?d1.
Step 4: Embed the ‘k’ sub pixel of each row of the share matrix ‘K’ into the k embedding positions chosen in Step2

The existing system is not fully secure. The shares should be sent through the Network and the Recipient will stack them up to get the original image [6]. If any attacker knows the logic behind the arrangement of shares they can easily retrieve the original image by overlapping the shares depending on Secure-Third-Party in the transmission phase. In this paper, we propose a new approach by key based visual cryptographic scheme. It improves the security principles like confusion, complexity and confidentiality which will given an added security to the data

The next part of the paper is organized in the following way. Section 2 describes the process of the existing system such as VCS. Section 3 consists of methodology of the proposed approach. Section 4 holds the results and analysis of the existing and proposed approaches. Performance evaluation by steganalysis is shown in section 5.

Related Work: In the process of Visual Cryptography Scheme (VCS) an input image has divided in to two shares as shown in the Fig. 1 [6]. The two shares (a) and (b) are distributed to two participants secretively, and no participant would get any information about the secret image except by stacking shares (a) and (b) [7].

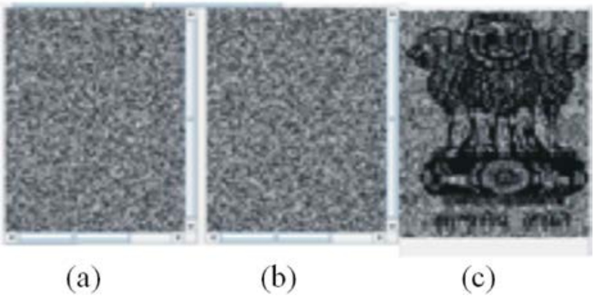


Fig. 1: Process of VCS

VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original objective (i.e., sharing secret image), have been found, for example, authentication and identification, watermarking and transmitting passwords etc.

Existing system Visual Cryptographic scheme (VCS) consists of modules such as Generating shares, generating overlaid images, and removing noise in the overlaid images [5]. In generating shares module, divides original data ‘N’ into ‘n’ pieces in such a way that ‘N’ can be easily reconstructed from any ‘k’ pieces, but even complete knowledge of any ‘k-1’ pieces reveals no information about ‘N’. Stacking two pixels (each consists of four sub-pixels) can occur for example in the following two cases: Secret sharing scheme is a method of sharing secret information among a group of participants [8]. In a secret sharing scheme, each participant gets a piece of secret information, called a share. When the allowed coalitions of the participants pool their shares, they can recover the shared secret; on the other hand, any other subsets, namely non-allowed coalitions, cannot recover the secret image by pooling their shares.

Visual Cryptography system specifies criteria that can be used to judge the operation of a system, rather than specific behavior [9]. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels. If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. This should be contrasted with functional requirements that define specific behavior or functions. The input image for generating shares can be in any Image format. The size of image depends on computational power for efficiency. The size (in terms of pixels) the key for encryption should be equal to or more than the size of Generated shares. The Key image should be in the PNG format.

Proposed System

Methodology: The main feature of the existing system is that a set of qualified shares is able to recover the secret image without any cryptographic knowledge and computation devices [10]. The unqualified set of shares generating the original image is theoretically impossible. The shares should be sent through the network and the recipient will stack them up to get the original image. Data attacks were more common in the process of transmission of data in the existing system. While the proposed system can reduce the attacks when images as data are transmitted through a medium [11]. For secure image data transmission, with some shared key, encrypt the original image shares and sent through the network as shown in Fig 2. Even by stacking the encrypted images shares by some third person will not generate the original image without having the idea on key image.

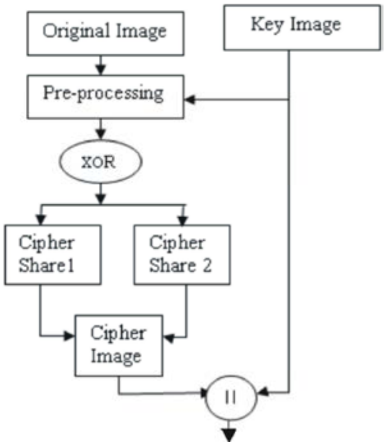


Fig. 2: Proposed System (KVCS) Process

The total process of the key based visual cryptography has shown as an algorithm 2.

Algorithm 2. Keyed Visual Cryptography Scheme Algorithm

1. Let us consider two input image files i. e Original data, Key data
   Let PI (Original Data) and KI (Key image) where KI= PI
2. Pre process them to get the shares.
3. Shares (PI), Shares (KI) _ Preprocessing
   PI1, PI2 _ Shares(PI), KI1, KI2 _ Shares (KI)
4. Generates Encryption shares i. e
   cipher share 1(EI1) and cipher share 2(EI2)
5. Make shares as a composite image i.e Cipher image (CI).
6. CI|| KI _ Receiver

Process of Encryption: As shown in fig 3, the original image is sent to VCS (Preprocessing system) where the original image is divided into two shares. The divided Key image has two partitions termed as key shares. In the encryption module, the original image shares were XORed with the corresponding key shares and generate the cipher shares such as Enc Img 1 and Enc Img 2 as shown in Fig 2. Then transmit the two encrypted shares with key image to the receiver.

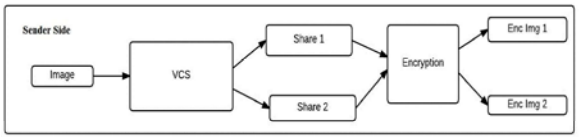


Fig. 3: KVCS Encryption Process

The process of Pre-processing and encryption of the shares of the image has shown as algorithm 3.

Algorithm 3. Encryption Algorithm

1. Divide an input image into two shares i.e PI1 and PI2.
2. Divide a Key image into two shares i.e KI1 and KI2.
3. Encrypt each share of the original image by key image share i. e Encrypt Image
   $PI1 \oplus KI1 \rightarrow EI\ 1$, $PI2 \oplus KI2 \rightarrow EI\ 2$
4. Generates Cipher Image.
   $EI1 \parallel EI2 \rightarrow CI$

Process of Decryption: In Decryption process, Cipher Image makes as shares i.e Enc Image 1 and Enc Image 2.

Simultaneously, Key Image which was received from the sender has been divided in to two shares. Apply logical operation XOR at Decryption module on Cipher Image shares and Key shares in order to get the original image shares. i. e share 1 and share 2 as shown in Fig 4. In the next phase Composite these two shares then finally get the original Image.

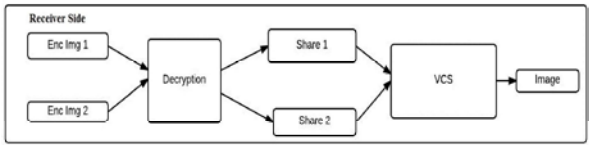


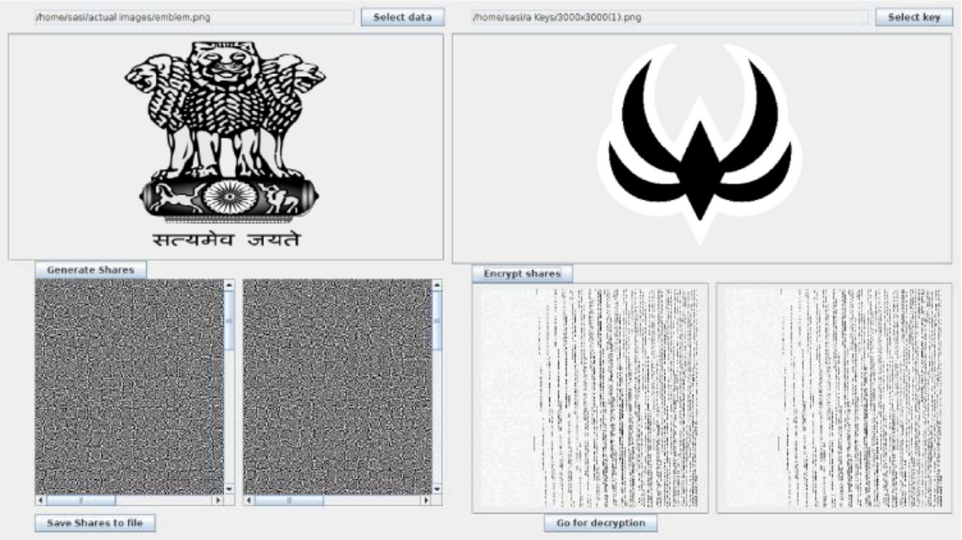
Fig. 4: KVCS Decryption Process

RESULTS AND ANALYSIS

Image data protection by KVCS, results are shown in Fig 5 and Fig 6 and Fig 7. Fig 5 shows the original Image (PI) decomposition as shares and encrypted shares by Key Image (KI).

Figure 6 shows the decryption process. It consists of the received cipher shares along with the shared key which are required to get the original Image (PI).

As a part of Decryption Process, extracting the original Image (PI) from encrypted shares by applying the reverse procedure of the encryption process is shown in Fig 7.


/home/sasi/actual images/emblem.png

/home/sasi/a Keys/3000x3000(1).png

Fig. 5: Shares generation

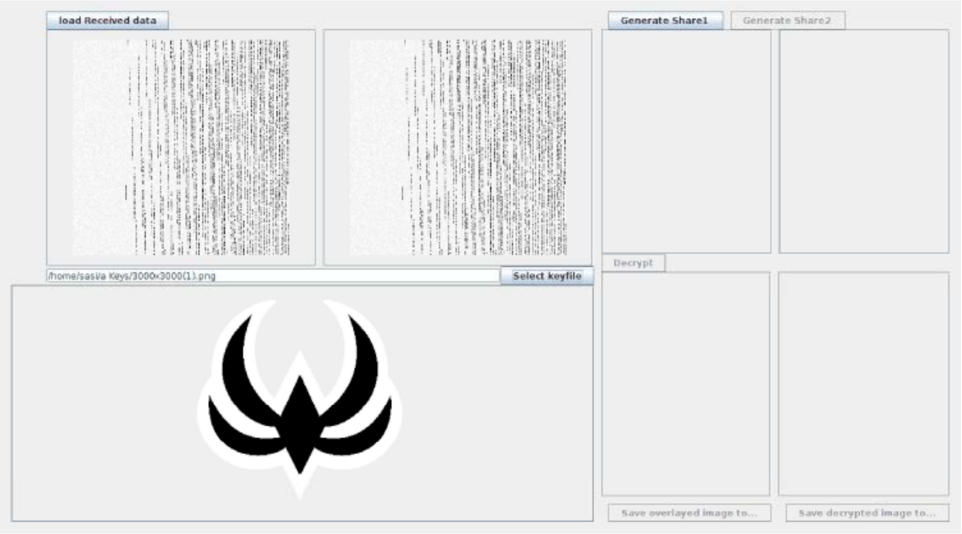

/home/sasi/a Keys/3000x3000(1).png

Fig. 6: Encrypted shares with Key

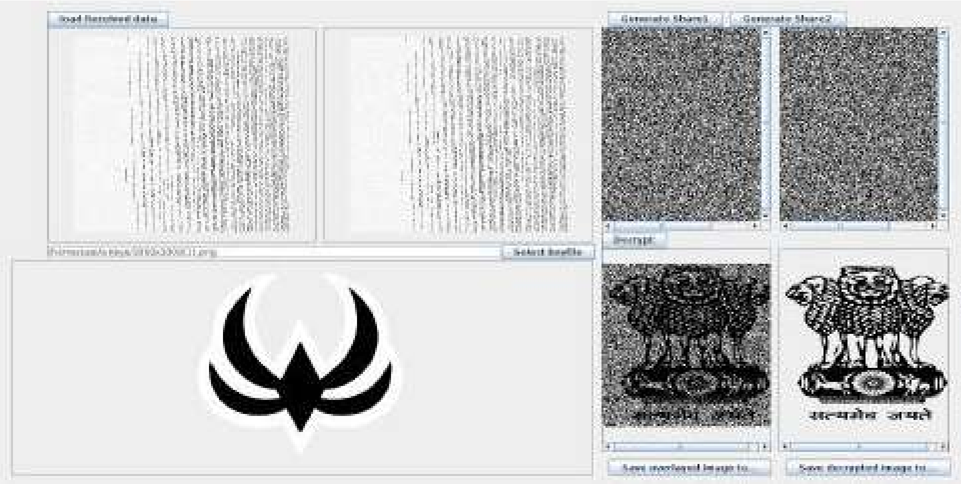


Fig. 7. Original Image from cipher shares (Enc Images)

Cryptanalysis:

The module “Generating Shares“ takes only binary image as input. The test case considered in the table 1, verified on three different input images. The test will pass for only Binary image. Other cases are failed.

Table 1: Cryptanalysis based on Original Input Image type

Description: Generating Shares For An Image.					
Preconditions: 1. Open the application. 2. Insert An Image.					
Steps	Test data	Expected Result	Actual result	Pass/Fail	Remarks
Select Original Image Path	Color Image	1.Image not accepted 2. Image accepted, should move to "Generate Shares" field	1. Image not accepted 2.Image accepted, should move to "Generate Shares" field	Fail	The Image should be Binary.
Select Original Image Path	Grayscale Image	1. Image not accepted 2. Image accepted, should move to "Generate Shares" field	1.Image not accepted 2. Image accepted, should move to "Generate Shares" field	Fail	The Image should be Binary.
Select Original Image Path	Binary Image	1.Image not accepted 2. Image accepted, should move to "Generate Shares"	1. Image not accepted 2.Image accepted, should move to "Generate Shares"	Pass	The Image should be Binary.

The module “ Encryption “ takes two inputs. One input is Generated share, and other input is key. The condition is that the key image size should be greater than the share. In the test case in table 2, two input images have been provided. The test will pass for only case 1, where the key size is more than the size of share. Other case is failed.

Table 2: Cryptanalysis based on Key

Description: Encrypt shares using a key					
Preconditions: 1. Open the application. 2. Insert An Image. 3. Generate shares					
Steps	Test data	Expected Result	Actual result	Pass/Fail	Remarks
Encrypt Shares using key image	1 Share 2 Key (key size more than the shares)	1. key not accepted 2. key accepted, should move to "send" field	key accepted, should move to "send" field	Pass	The key size is greater than shares
Encrypt Shares using key image	1 Share 2 Key (key size less than the shares)	1. key not accepted 2. key accepted, should move to "send" field	1.Key not accepted	Fail	The key size should be greater than shares

The module “Decryption “takes two inputs. One input is Encrypted share, and other input is key. The condition is that the key image size should be greater than the Encrypted share. Table 3, shows the test results of two input images taken into consideration. The test will pass for only case 1, where the key size is more than the size of Encrypted share. Other case is failed

Table 3: Cryptanalysis based on Encrypted shares

Description: Decrypt shares using a key					
Preconditions: 1. Open the application. 2. Insert An Image. 3. Generate shares 4. Encrypt shares Send					
Steps	Test data	Expected Result	Actual result	Pass/Fail	Remarks
Decrypt Shares using key image	1 Encrypted Share 2 Key(key size more than the encrypted shares)	1.key not accepted 2.key accepted, should move to "overlay" field	key accepted, should move to "overlay" field	Pass	The key size is greater than Encrypted shares
DecryptShares using key image	1 Encrypted Share 2 Key(key size less than the encrypted shares)	1. key not accepted 2.key accepted, should move to "Overlay" field	1. key not accepted	Fail	The key size should be greater than Encrypted shares

CONCLUSION

Visual Cryptography is a creative technique of sharing cryptic/covert data. It is generally used either for sharing any secret among individuals or is used for authentication purpose. It can be used in different fields and different areas to ensure security. this technique when it is used over internet, the shares should be sent through the Network and the Recipient will stack them up to get the original image. For secure transmission we should rely on secure-third-party. The original image which should be shared covertly will be encoded in two shares. With some shared key we will encrypt the shares of the original image and sent through the network. Even stacking the encrypted images by a third person will not generate the original image. Recipient should decrypt the encrypted images with the same shared key to generate the shares. Then recipient will stack them to get the original image.

REFERENCES

1. Dhiraj Pandey, Anil Kumar and Yudhvir Singh, 2013. Feature and Future of Visual Cryptography Based Schemes’, 9th International Conference, QShine 2013, Springer, LNICS, pp: 816-830.
2. Feng Liu, Teng Guo, ChuanKun Wu and Ching-Nung Yang, 2014. Flexible Visual Cryptography Scheme and Its Application’, Transactions on Data Hiding and Multimedia Security IX, Lecture Notes in Computer Science Volume 8363, pp: 110-130.
3. Arumugam, S., R. Lakshmanan and Atulya K. Nagar, 2014. On (*k*, *n*)*-visual cryptography scheme’, Designs, Codes and Cryptography, 71(1): 153-162.
4. Ch, Rupa, 0000. “A Novel Approach in Security using Gyration Slab with Watermarking Technique”, Springer IEI, 2015. 10.1007/s40031-015-0195-3.
5. Ch. Rupa, 2013. Digital Image Steganography using Sieperinski Gasket Fractal and PLSB, Springer IEI, Vol 54, issue 3. 2013
6. Naskar P., A. Chaudhuri and Chaudhuri Atal, 2010. Image Secret Sharing using a Novel Secret Sharing Technique with Steganography’, IEEE CASCOM, Jadavpur University, pp: 62-65.
7. Yasushi Yamaguchi, 2012. An Extended Visual Cryptography Scheme for Continuous-Tone Images, Digital Forensics and Watermarking Lecture Notes in Computer Science 7128: 228-242.
8. Divya James and Mintu Philip, 2012. A Novel Security Architecture for Biometric Templates Using Visual Cryptography and Chaotic Image Encryption, Eco-friendly Computing and Communication Systems Communications in Computer and Information Science, 305: 239-246.
9. Feng Liu, Wei Q. Yan, Peng Li and Chuankun Wu, 2013. A Secret Enriched Visual Cryptography, Digital Forensics and Watermaking, Lecture Notes in Computer Science, 7809: 464-484.
10. Liu, F., C.K. Wu and X.J. Lin, 2009. The alignment problem of visual cryptography schemes, Designs, Codes and Cryptography, pp: 215-227.
11. Shamir, A., 1979. How to share a secret, Communications of the ACM 22: pp: 612-613.
12. Yang, C.N. and C.B. Ciou, 2010. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability’, Image and Vision Computing, 28: 1600-1610.