International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 13 (2018) pp. 11340-11343

Role of Visual Cryptography Schemes in Information Security: A Review

Suresh Prasad Kannojia and Jasvant Kumar

ICT Research Lab, Department of Computer Science,
University of Lucknow, Lucknow-226007, UP, India.

Abstract

To secure important information, different techniques are used. Traditional cryptography is playing an important role to do this work. Security through a typical cryptographic system, relies on certain keys along with the complex encryption and decryption algorithm. Thus, the security of information mainly depends on security of key due to which, rely on the information kept on a single channel (person, physical entity etc.) is not secure. These problems are elegantly controlled by visual cryptography schemes. This paper has focused on the role of visual cryptography schemes in information security as well as the details of different situations for which the use of traditional cryptography is not appropriate. Finally, we find that visual cryptography schemes have increased the information security.

Keywords: Cryptography, Information Security, Visual Cryptography, Secret Sharing, Visual Secret Sharing

INTRODUCTION

With the current era of electronic commerce, there is an urgent need to ensure the security of information in growing open network environment. Generally, encryption techniques such as DES, AES, and ECC are used for information security. In the cryptographic technologies, data becomes disordered after encryption phase. To retrieve the data, we require large quantities of computation with the complex decryption algorithm and right keys. Also to retrieve original data from encrypted data without the correct key is very difficult. If adversaries get secret key by any mean they can retrieve the message without longing. Thus, the security of information mainly depends upon the security of the key. If too many copies of secret key are created and distributed, one of the key holders might go away from the right path or if too few copies are created, that all might be destroyed. These problems are separately studied by G.R. Blakely [1] and A. Shamir [2]. According to G. R. Blakley, security of the key is needed due to cause of abnegation, betrayal and combinational incident. Shamir presented how to share secret between two or more people or channels without breaking the confidentiality of the message. It is based on polynomial interpolation, requires computation to retrieve messages while ensures confidentiality of the key. Shamir divided the key into two or more parts, each part given to separate person. Parts of the key given to an individual convey no any information about original key. Visual cryptography [3] is a secret sharing technique which facilitates the security of information. It neither requires complex encryption, decryption algorithms nor large amount of computing power to retrieve the secret information. Visual cryptography basically divides key message (in image form) into two or more noise-like images. These noisy images are known as shares and distributed to the same number of participants in such a way that each participant receives only one share. Individual share conveys no clue about the original secret message. Secret message can be retrieved by the human visual system by stacking shares printed on transparencies. This allows us to decode secret without the knowledge of cryptography. Besides, solutions to key sharing other applications of visual cryptography are in information hiding [5], authentication and identification [6], watermarking [7], and transmitting passwords [8], copyright protection [9] etc. This paper includes description about information security, conditions in which security of key required and description of a basic visual cryptography scheme with analysis followed by conclusion.

INFORMATION SECURITY

Successful organizations have multiple layers of security in place to fulfill their objectives. It covers physical, personnel, operations, communications, networks and information security. Information security is a subset of security. It begins with the computer security. The Committee on National Security System (CNSS) [10] defines information security as the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information, to ensure confidentiality, integrity and availability. To fulfill the objectives, organizations have to protect every asset of the organization, but confidentiality of information plays a major role for successful implementations of organization's objective.

SITUATIONS UNHANDLED BY TRADITIONAL CRYPTOGRAPHY

In order to secure data, encryption techniques have been used. It means security of data directly depend on security of key. To secure encryption key, we need another way because due to the encryption of the keys, the problem increases rather than solve it. Existing secure key management schemes, keeps them on a single channel (computer, person, locker). These schemes are not suitable because a single misfortune (computer breakdown, sudden death, sabotage), can lead to inaccessibility of the key. Thus, relying on a single channel is not good habit. Solution to the problem is that; keep multiple copies of the key in different places, but this leads to security breaches (computer hacking/penetration, betrayal or human errors). Suppose a typical cryptosystem have a number of copies of vital information in protected memory locations. There is possibility of destruction of vital information if any

act to do so occurs. Since an opponent will try to destroy the system by an act of tempering to the vital information. Now the question is that, what are the incidents in which key information needed to be guarded? The answer to the question is given by G.R Blakley [1]. These are abnegation, betrayal and combinational incidents. Descriptions about these incidents are given bellow.

Abnegation Incidents

An incident after which piece of information is not reclaimable by the organization from the person holding the key information because of:

Destruction

Key information may be destroyed because person carrying key information can be a victim of unexpected accidental incident.

Degradation

Holder of key presents a copy of the other key rather than the right key due to confusion or embarrassment.

Defection

A person who has a copy of important information can appear in front of the opposition and refuse to tell the organization that was given to keep it safe.

Betrayal Incidents

Betrayal incident is a situation after which key information is completely known to adversaries of the organization. There are mainly two types of incidents.

Defection

We have already encountered in the category of abnegation incidents.

Dereliction

An act in which custodian of the key reveals key to adversaries and still behaves like an honest personnel for the organization which entrusted to him. For example, the person who has the copy of the key can show it to adversaries, but still plays the part of a faithful guard, and even report the key information back correctly when requested.

Combinational Incidents

Combinational incidents are combination of abnegation and betrayal incident. Defection is an example of combination incidents.

From the description about different type of incidents given above, it is clear that, except in destruction incident, in all other incidents confidentiality of the information breaches. Custodian of keys has shared information about key with the adversaries of the organization. In the case of destruction, the key is destroyed due to unexpected accidental incidents. The majority of incidents is happening due to confidentiality breaches. It means confidentiality of information play major role in information security.

VISUAL CRYPTOGRAPHY

This section presents details on visual cryptography with experimental results and analysis.

Model

Suppose, S be a binary secret image and P = $\{p_1, p_2...p_n\}$, be a set of n participants, among which secret image will be shared. Let, 0(1) represents white (res. black) pixels. Each pixel of the secret image handled separately. When we will share pixels of the secret image. Each pixel of secret image will appear in n modified version (shares), one for each participant. To do so, we need $m \geq n$ auxiliary pixels for every original pixel, where m is a collection of black and white sub-pixels. Arrange shares for pixels in such a way that resulting structure is an $n \times m$ Boolean matrix $M = [b_{i,j}]_{n\times m}$, where $b_{i,j}$= 1 if j^{th} sub-pixel of i^{th} share is black. When shares $i_1,i_2,...i_r$ are printed on transparencies and stacked with proper sub-pixel alignment we see a combined transparency whose black sub-pixels are represented by Boolean 'OR' of the rows $i_1,i_2,...i_r$ in M. Gray-level of this resultant transparency is directly proportional to the hamming weight $H_w(V)$ of the "OR"ed, $m-$vector V . This gray-level of combined transparency interpreted as black by human visual system if $H_w(V) \geq t$ and white if $H_w(V) < t - \alpha \times m$, $1 \leq t \leq m$ and $\alpha > 0$. Parameters t and α, are used to distinguish colors. Formal definition of this scheme is given bellow.

Definition 1[3] Two collections of n × m Boolean matrices C^0 and C^1 have a valid solution to the problem of k-out-of-n or (k, n) visual cryptography scheme if, following three conditions are satisfied.

1. For any M in C^0, "OR"ed vector V of any k out of n rows satisfies that $H_w(V) \leq t - \alpha \times m$.
2. For any M in C^1, "OR"ed vector V of any k out of n rows satisfies that $H_w(V) \geq t$.
3. For any subset $\{i_1,i_2,...i_r\}$ of {1,2,...n} with r < k, two collections of r × m matrices D^γ, $\gamma \in \{0,1\}$, obtained by restricting each matrix in C^γ, $\gamma \in \{0,1\}$ to rows $i_1,i_2,...,i_r$ are indistinguishable in the sense that they contain the same matrices with same frequencies.

First two conditions for security while condition third for contrast. Parameters used in the scheme are defined as follows

Definition 2 (m) m is defined as number of sub-pixels needed to encode a single black or white pixel of the secret image

Or

Ratio of resolution of a generated share or reconstructed image to the original secret image is called as pixel expansion. It represents scaling in original secret image. Objective of visual cryptography scheme is that it should be as small as possible.

Definition 3 (α) Let h_w and b_w represents hamming weight of white and black pixels in reconstructed image in respect of original secret image then α is defined as

$$\alpha = \frac{b_w - h_w}{m} \quad (1)$$

It, represents loss in contrast. Objective of visual cryptography scheme is that it should be as large as possible. Original secret message will retrieve whenever value α of become equal to one.

Definition 4 (t) Threshold value t is used to differentiate between white and black colors in the reconstructed image. If in the collection of m sub-pixels number of black pixels is less than or equal to t then human visual system interpenetrates collections of m pixels as white color else black.

Illustration with Experiment

Experimental results for basic visual cryptography scheme for two participants with *m* = 2 using MATLAB are shown in Figure 1. Here, it is obvious that to encrypt white (resp. black) pixel one of the two available options can be chosen randomly.

Basis matrices M_0 and M_1 are created using the shares of white and black pixels respectively. Rows of the M_0 in row R_1 is corresponding to shares for white pixel in R_1. Similarly, basis matrices corresponding to R_2, R_3 and R_4 are generated.

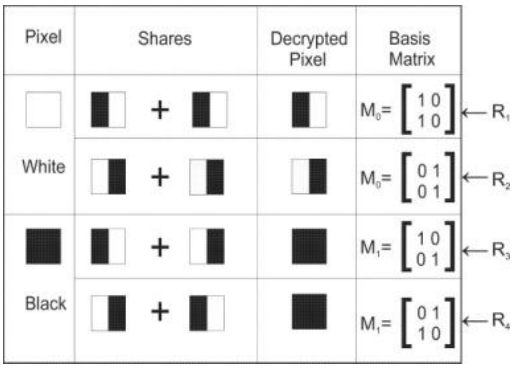

Figure 1: Basic 2-out-of-2 Visual Cryptography scheme with m = 2

It is clear that shares in Figure 2 are random-noise like two dimensional patterns of black and white pixels. Individual shares have no clue about the secret image.

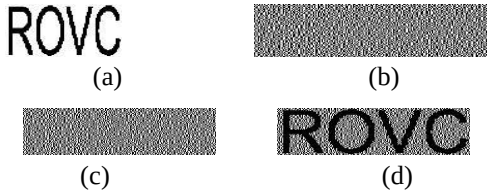

Figure 2: Example of 2-out-of-2 visual cryptography scheme with *m* = 2 (*a*) Secret image (*b*) and (*c*) are Shares (d) Reconstructed Secret image

To reveal secret image shares are printed on transparencies and aligned properly and viewed by human visual system

Analysis

Analysis is based on basic visual cryptography scheme illustrated with experimental results in section illustration with experiment. From description and experimental results, it is very clear that visual cryptography scheme consists of three main steps. First one is construction matrix generation. Second one is creation and distribution of shares and finally reconstruction of secret image. Construction or basis matrices basically depend on number of participants and pixel expansion. In the given visual cryptography scheme basis matrices for two participants with *m* = 2 are generated. To divide secret image into more than one shares an encryption algorithm is needed along with basis matrices for white and black pixels. Based on the color of secret image, encryption algorithm selects one of the available basis matrices for that pixel and generates shares. Overall process of visual cryptography scheme is shown in table 1. Let 0 be white pixel of the secret image and chosen basis matrix is $\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$. Encryption algorithm assign rows of the basis matrix to the participant S_1 and S_2 are 1 0 and 1 0 are respectively. "OR" ed m-Vector V of shares assigned to S_1 and S_2 is 1 0. Hamming weight $H_w(V)$ of "OR" ed m-Vector V is 1. By the human visual system it is interpreted as white (partial) because threshold value (t) is 1. After carrying out this process for every pixel of secret image experimental results shown in Figure 2. From that, it is clear that share images are random noise like two dimensional patterns of black and white pixels having no clue about the secret image. Therefore, no one can decode the secret from a single share image even if he is given infinite computing power to do so. To reconstruct the secret image just print shares on transparencies and stack them, aligned pixel-wise carefully. This mechanical operation is just like pixel-wise OR operation between the shares. Shares are assigned to participants one by one. Since, shares have no clue about the secret image so custodians of the shares are not able to breach the confidentiality of secret (key). In the case of destruction, consider a (k, n) visual cryptography scheme with k=2 and n>3. In this scheme, secret is shared between three participants in such a way that if any one participant meets to unexpected accident, other two participants can decode secret jointly

Table 1: Working Process of Visual Cryptography Scheme

Secret Pixel	Basis Matrix	S_1	S_2	"OR" ed m-Vector V	$H_w(V)$	Reconstructed Pixel
0	$\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$	1 0	1 0	1 0	1	Partial white
0	$\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$	0 1	0 1	0 1	1	Partial white
1	$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	1 0	0 1	1 1	2	Black
1	$\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$	0 1	1 0	1 1	2	Black

.

CONCLUSION

Visual cryptography scheme divides important information into multiple parts and keep them on different channels. Any individual part conveys nothing about the original information. Participant of the key, willingly or unwillingly are not able to breach confidentiality of the key. It means visual cryptography enhances security (confidentiality) in all the conditions of abnegation, betrayal and combination incidents. Unlike the traditional cryptography decryption process of visual cryptography technique needs minimum computational requirement without complex decryption algorithm.

ACKNOWLEDGMENT

This work was supported by University Grant Commission, India (RGNF award No: F1-17.1/2014-15/RGNF-2014-15-SC-UTT-87345/ (SAIII/Website))

REFERENCES

[1]. Blakley, George Robert., 1979 "Safeguarding cryptographic keys." *Proceedings of the national computer conference*. Vol. 48.

[2]. Shamir, Adi., 1979 "How to share a secret." *Communications of the ACM*, 22.11, 612-613.

[3]. Naor, Moni, and Adi Shamir., 1995 "Visual cryptography." *Advances in Cryptology? EUROCRYPT'94*. Springer Berlin/Heidelberg.

[4]. Stallings, William, and Mohit P. Tahiliani., 2014 *Cryptography and network security: principles and practice*. Vol. 6. London: Pearson.

[5]. Yan, Xuehu, et al., 2015 "New approaches for efficient information hiding-based secret image sharing schemes." *Signal, Image and Video Processing*, 9(3), 499-510, 2015.

[6]. Naor, Moni, and Benny Pinkas., 1997 "Visual authentication and identification." *Advances in Cryptology-CRYPTO'97, 17th Annual International Cryptology Conference*, Santa Barbara, California, USA, August 1997. Proceedings. Springer Berlin/Heidelberg

[7]. Chen, Tzung-Her, and Du-Shiau Tsai. 2006 "Owner? Customer right protection mechanism using a watermarking scheme and a watermarking protocol." *Pattern Recognition* 39(8), 1530-1541.

[8]. Tuyls, Pim, et al., 2004 "Visual crypto displays enabling secure communications." *Security in Pervasive Computing*. Springer, Berlin, Heidelberg, 271-284.

[9]. Chang, Chin-Chen, and H. C. Wu., 2001 "A copyright protection scheme of images based on visual cryptography." *The Imaging Science Journa*l 49(3), 141-150.

[10]. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec) Professionals. 20 June 1994. File, 4011.