International Journal of Research in Advent Technology, Vol.2, No.5, May 2014
E-ISSN: 2321-9637

Visual Cryptography: Keyless Approach for Image Encryption

Ms. Kirti Mhamunkar [1,] Mrs Smita Deshmukh [2]
Information Technology, Mumbai University
Email: kirtimhamunkar@gmail.com [1]

Abstract- Visual Cryptography is a technique that allows information (images, text, diagrams) to be encrypted using an encoding system that can be decrypted by the eyes. Visual cryptography provides a very powerful and secure technique by which one secret can be distributed into two or more shares. When the shares are xeroxed onto transparencies and then superimposed exactly together, the original secret can be discovered without computer participation. In VC generate random shares such that with minimal computation, the original secret image can be recovered from the random shares without any loss of image quality. Intent of this paper is dividing the image into random shares to maintain the images secrecy. SDS algorithm is used for image encryption without keys.

.

Index Terms- Visual cryptography, encryption, decryption, contrast, security, accuracy, computational complexity.

1. INTRODUCTION

Visual Cryptography is first introduced by Moni Naor and Adi Shamir, in 1994. In this show how to split a secret message into two components. Both parts are necessary to reconstruct and reveal the secret, and the possession of either one, alone, is useless in determining the secret.

Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.[1]They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image.

Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear [3]Visual cryptography encodes a secret binary image into n shares of random binary patterns. The secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset [2] Encryption is the first process in which the plain text or readable text is converted into cipher text or unreadable text.

The second process is called decryption process in which cipher text or unreadable text us converted into plain text or readable text.

To encrypt data we apply an encryption algorithm at the sender end and to reveal the data at the receiving end, we apply a decryption algorithm. But we need to consider the situation where there is no option to use the decryption process. The most notable feature of this approach is that it can recover a secret image without any computation.[5]

2 .PROPOSED TECHNIQUE

Proposed technique is splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required.

The proposed technique is implemented with the SDS algorithm and involves three steps.

Step 1- (Sieving) the secret image is split into primary colors.

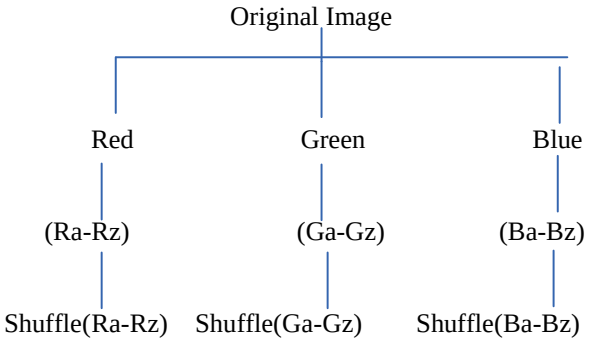
Step 2 (Division) these split images are randomly divided.

Step 3 -(Shuffling) these divided shares are then

shuffled each within itself. Finally these shuffled shares are combined to generate the desired random shares. [4]

Step 1 (Sieving) : Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components The granularity of the sieve
depends the range of values that R/G/B component may take individually. To make the process computationally
inexpensive, sieving uses the XOR operator. Representation of the Sieving operation

Division: Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.



Random Share A **Random Share 2**

Step 2 (Division): Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.[4]

R =(RA, RB, RC,----------, RZ)

G = (GA, GB, GC,----------, GZ)

B = (BA, BB, BC,----------, BZ)

Step 3 (Shuffling): It involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary color.

Algorithm
1. Sieving
Input Æ Secret Image
Sieve(Secret Image)
Output Æ(R, G, B components)
2. Division
n = total number of pixels (0 to n-1)
Ri / Gi / Bi = individual values of the ith pixel in the R, G, B components

z = total number of random shares

x =number of bits representing each primary color
max_val = 2x
Repeat 2 for R, G, B component
2(a) for i = 0 to (n-2)
{ for share k = A to (Z-1)
Rki = Random(0, max_val)
Aggr_Sumi = ™ Rki
}
Rzi =(max_val + Ri – (Aggr_Sumi % max_val)) % max_val
3. Shuffle
Repeat for RA-Z, GA-Z and BA-Z (all generated shares)
for k = A to Z
{ Rk-shuffle = Rk
PtrFirstVac = 1
PtrLastVac = n-1
For i = 1 to (n-1)
{ If (R(k+1)(i-1) is even)
{ R(k-shuffle) PtrFirstVac = Rki
PtrFirstVac ++, i++
}
Else
{ R(A-shuffle) PtrFirstVac = RAi
i++, PtrLastVac --
} } }
4. Combine
For k = A to Z
RSk = (Rk-shuffle XOR Gk-shuffle XOR Bk-shuffle)

Thus at the end of the above process we have Random

shares (RSA ,RSB ---------- Rsk).

In proposed scheme there are no keys involved and hence there is no key management. All that is required is to transmit one of the random shares on a secret channel while transmitting the rest on an unsecure channel. This schema is also using when the CMY or the subtractive model, the colors are represented by the degree of the light reflected by the colored objects. In this scheme Cyan (C) Magenta (M) and Yellow (Y) pigments are used to produce the desired range of colors. For decryption purpose XOR operation is used.

The decoding step involves use of a weighted matrix B generated during the training phase and a seed ‘s’ used in the encryption phase, thus handling of

these two secret elements raises issues similar to key management in an encryption algorithm.

3. CONCLUSION AND FUTURE SCOPE

In this paper a new enhanced visual cryptographic scheme is introduced, In which s secret image is split into multiple random images and with minimum computation the original secret image can be retrieved back. Key management is not an issue because no encryption keys are used, Computation cost is low. This is best way keyless approach for image encryption.

Future work for this we can use Compression of encrypted shares to reduce bandwidth requirement.
And also take Size of image Variations in format of Input image.

REFERENCES

[1] Survey of Visual Cryptography Schemes-nternational Journal of Security and Its Applications Vol. 4, No. 2, AprilApril,ril, 2010

[2] Zhi Zhou; Arce, G.R.; Di Crescenzo, G., "Halftone visual cryptography," Image Processing, IEEE Transactions on , vol.15,no.8, pp.2441,2453, Aug. 2006.

[3] Moni Naor and Adi Shamir, ”Visual cryptography”, in Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer-Verlag, 1994.

[4] Siddharth Malik, Anjali Sardana ”A Keyless Approach to Image Encryption”2012 International Conference on Communication Systems and Network Technologies

[5] Asmita Kapsepatil, S. L. Varma”Analysis on Visual Cryptography for Color Image with Error Diffusion “(IJEIT) Volume 2, Issue 1, July 2012

[6] Akerkar, R. A.; Lingras, P. (2008). *An Intelligent Web: Theory and Practice*, 1st edn. Johns and Bartlett, Boston.

[7] Albert, R.; Jeong, H.; Barab´asi, A.-L. (1999): Diameter of the world-wide Web. Nature, **401**, pp. 130–131.

[8] Berry M. W., Dumais S. T., O’Brien G. W. (1995): Using linear algebra for intelligent information retrieval, SIAM Review, **37**, pp. 573-595.

[9] Bharat, K.; Broder, A. (1998): A technique for measuring the relative size and overlap of public Web search engines. Computer Networks, **30**(1–7), pp. 107–117.

[10] Broder, A.; Kumar, R.; Maghoul, F.; Raghavan, P.; Rajagopalan, S.; Stata, R.; Tomkins, A.; Wiener, J. (2000): Graph structure in the Web. Computer Networks, **33**(1–6), pp. 309–320.

[11] Chakrabarti, S. (2000): Data mining for hypertext: A tutorial survey. SIGKDD explorations, **1**(2), pp. 1–11.