ISSN:0975-9646

Assorted Image Based Obscure Techniques In Visual Cryptography

Thanuganesh.M*
PG scholar
Dr.N.G.P.Institute of Technology
Coimbatore, India.

Saranya.R
Assistant Professor
Dr.N.G.P.Institute of Technology
Coimbatore, India.

Abstract: With the unpredictable growth of internet and the fast transmission techniques in recent years the security and the privacy of the sensitive data has become of prime concern. To protect this data from illegal access and tampering various methods for data obscure like visual cryptography, stenography, authentication have been developed our environment. In this survey we will be discussing one such data obscure technique called visual cryptography. Visual cryptography is the process of obscure important information in any variant media to transfer it securely over the underlying unreliable and unsecured communication media by the usage of different image types like digital image, natural image, grey image. This survey on various data obscure techniques in cryptography that are in practice today along with the comparative analysis of these techniques.

Index Terms— visual cryptography, obscure techniques, images.

1.INTRODUCTION:

Entitled to massive evaluations in Internet it is a real challenge to keep secret information obscure. The web services are now almost open to everyone and that is why the prospect of reaching sound data from one system to another system or from one user to another user may not be safe at all. Before sending data it must be encoded first. If it can somehow be managed to encode the information and then send it, safety can be assured up to a fair extent. In this survey proposed to encode the information which cannot be decode without a proper generated share.

Visual cryptography scheme is an encryption scheme that was able to encrypt an information using images that suggested by Naor and Adi Shamir [1]. It is a type of cryptography in which images can be securely encrypted by dividing them in a deformed image called transparent shares and transmitted through physically by printing these shares on transparency sheets to the intended user. This survey on various data obscure techniques using variant of images like grey-scale images, digital images, natural images, RGB images.

2. ASSORTED IMAGES:

2.1*grayscale Image*

Grayscale image[2], the intensity value is taken to represent height above a root plane, the grayscale image represents a surface in three-dimensional Euclidean space. Figure1 shows such a surface. Then the set of coordinates associated with this image surface is simply the set of three-dimensional Euclidean coordinates of all the points within this surface and also all points below the surface, to the root plane[2]. Observe even when we are only considering points with numbered coordinates, this is a lot of points, more algorithms are employed that do not need to consider all the points.

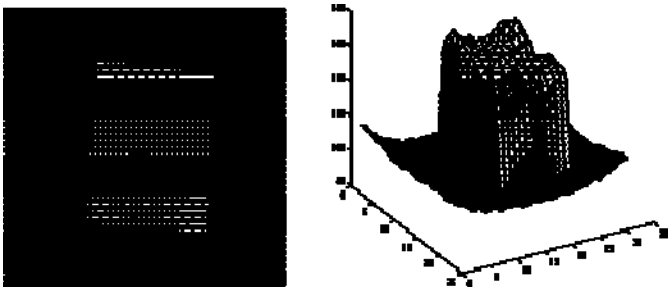

Figure 1

2.2*digital Images*

A digital image[3] is a numeric representation of a 2D image. Subject on whether the image resolve is fixed, it may be of vector or raster type. By itself, the term "digital image"[3] usually refers to raster images or bitmapped images. Figure2 shows such a surface .Improvement of pictorial information for human interpretation Processing of image data for store, transmission and representation for autonomous machine perception.

Figure 2

2.3*color Images:*

A **color image[4]** is a digital image that includes color information for each point. For visually acceptable results, it is necessary to provide three samples (color channels) for each point, which are interpreted as coordinates in some color space. Color area of RGB is commonly used in system displays, but other area such as HSV, YCbCr, and are often used in other contexts. A color image[4] has three values per point and they measure the intensity and chrominance of light. The original information stored in the digital image data is the brightness information in each spectral band. Figure3 shows such a surface.

Figure 3

2.4*natural Image:*

Natural image[5] refers to the process by which an agent (such as a human paintings, drawings) visually takes in and interprets scenes that it typically encounters in natural modes of operation (e.g. busy streets, meadows, living rooms). This process has been modeled in several different ways that are guided by different concepts. Figure4 shows such a surface.

Figure 4

3.VARIOUS OBSCURE TECHNIQUES

3.1 *Visual Cryptography*

Visual cryptography[1] is a cryptographic technique which allows visual information (pictures, text, etc.) to be encoding in such a way that decoding becomes a mechanical operation that does not require a computer. In 1994 best-known techniques has been credited to Moni Naor and Adi Shamir, who developed visual cryptography. Noar and Shamir demonstrated a visual secret sharing scheme, where an image was divide up into n splits so that only someone with all n splits could decrypt the image, while any n − 1 splits revealed no information about the original image. Every split was printed on a separate slide, and decoding was performed by plated the splits[1]. When all n splits were plated, the original image would appear. Same idea, slide can be used to implement a one-time pad encoding, where one slide is a split random pad, and another slide acts as the cipher text.

3.2 *Extended Visual Cryptography*

An extended visual cryptography scheme (EVCS) was proposed by Ateniese[5] . Extended visual cryptography schemes permits the construction of sharing images within which the splits are meaningful as opposed to having random noise on the splits. After the sets of splits are superimposed, this meaningful data disappears and the secret is recovered[5]. This is the basis for the extended form of visual cryptography.

3.3 *Image Size Invariant Visual Cryptography*

The image size indifferent visual cryptography[4] was proposed by Itoet . The traditional visual cryptography method employ pixel . In pixel extension, each share is m times the size of the secret image. Thus, it can lead to the difficulty in carrying these shares and consumption of more storage space. Ito's method removes the need for this pixel extension. That is, the reconstructed image is identical to the original image[4]. There are also some other studies which focus on the methods without pixel extension

3.4 *Recursive Hiding*

This provides a method of hiding secrets recursively in the shares of threshold schemes, which permits an efficient utilization of data. In recursive hiding of secrets, several additional messages can be hidden in one of the shares of the original secret image[9] . By using recursive threshold visual cryptography in network application, network load can be reduced.

3.5 *Color Visual Cryptography*

VCS schemes is that the number of colors and the number of sub pixels determine the resolution of the revealed privacy image[6]. So many colors are used, the sub pixels require a large matrix to represent the privacy image. The contrast of the revealed secret image will go down drastically. Consequently, how to correctly stack these shared slide and recognize the revealed secret image are the major problems. The assorted color visual cryptography schemes are studied in . Almost all color visual cryptography schemes proposed required few calculations.

3.6 *Natural Image–Based Visual Cryptography*

NVSS scheme can split a digital secret image[8] overn 1 arbitrary natural images and one split. Replacement for altering the contents of the natural images, the current approach extracts features from each natural split. Slide unaltered natural splits are totally diverse, thus schme reducing the interception probability of these splits. The generated split that is noise-like can be concealed by using data hiding techniques to increase the security level during the transmission phase.

4. COMPARISON OF ASSORTED IMAGES AND OBSCURE TECHNIQUES

Hiding Techniques	Pixel Extension	Assorted Format	Type of split Generated
Visual cryptography	4	Digital	Random
Extended visual cryptography	3n	Grey level	Meaning full
Imagesize invariant visual cryptography	1	Digital	Random
Recursive hiding	C*3	Color and grey scale	Random
Color visual cryptography schemes	C*9	Color	Random
Natural image–based visual cryptography	529	Natural color image	Meaning full

CONCLUSION

The developments and proposals by different models in visual cryptography schemes are reviewed here. The different perspectives on visual cryptography such as types of assorted images, different techniques, and color models of secret images etc. are discussed in this chapter. The construction of basis models visual cryptography, extended visual cryptography, color visual cryptography for is demonstrated with examples. The consistent image size visual cryptography scheme has also been explained with example.

REFERENCES

[1] M. Naor and A. Shamir, ―Visual cryptography,‖ in *Advances in Cryptology*, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, ―Incrementing visual cryptography using random grids,‖ *Opt. Commun.*, vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[3] P. L. Chiu and K. H. Lee, ―A simulated annealing algorithm for general threshold visual cryptography schemes,‖ *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[4] K. H. Lee and P. L. Chiu, ―Image size invariant visual cryptography for general access structures subject to display quality constraints,‖ *IEEE Trans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, ―Extended capabilities for visual cryptography,‖ *Theoretical Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] I. Kang, G. R. Arce, and H. K. Lee, ―Color extended visual cryptography using error diffusion,‖ *IEEE Trans. Image Process.*, vol. 20, no. 1, pp. 132–145, Jan. 2011.

[7] F. Liu and C. Wu, ―Embedded extended visual cryptography schemes,‖ *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[8] Lee and Chiu: Digital image sharing by diverse image media ―ieee transactions on information forensics and security, vol. 9, no. 1, january 2014