International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data Sharing through Multimedia Steganocryptic and Visual Cryptography System

Gajangi Rahul Kumar[1], U .Shivaji[2]

[1]M.Tech(Student), CSE Department, St Martin's Engineering College, Dhulapally, Secunderabad, Telgana, India-500014

[2]Associate Professor, CSE Department, St Martin's Engineering College, Dhulapally, Secunderabad, Telgana, India-500014

Abstract: ***The Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme that fixates on sharing secret images. The fundamental conception of the visual cryptography scheme is to split a secret image into number of desultory shares (printed on transparencies) which discretely reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the portions. In the multimedia steganocryptic system, the message will first be encrypted utilizing public key encryption algorithm, and then this encrypted data will be obnubilated into an image file thus accomplishing both data encoding and obnubilating. The multimedia data will be acclimated to provide the cover for the information. Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. In this paper concept of visual cryptography is discussed which is an impeccably secure method of keeping images secret, for feasible use in biometric identification technique and auspice such as dactylogram images for the purpose of utilizer authentication along with sundry visual cryptography schemes as an literature review. This paper not only reviews how to apply sharing of single secrete image and multiple secrete image on ebony and white as well as on color images but withal a comparative analysis on sundry visual cryptography schemes is withal performed.***

Keywords: Visual Cryptography Scheme (VCS), Random shares, steganocryptic system, Data encoding, biometric

1. Introduction

In today's information age, information sharing and transfer has incremented exponentially. The threat of an intruder accessing secret information has been an ever subsisting concern for the data communication experts. Cryptography and steganography are the most widely used techniques to surmount this threat. Cryptography involves converting a message text into an unreadable cipher. On the other hand, steganography embeds message into a cover media and obnubilates its subsistence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerably susceptible to intruder attacks. Albeit these techniques are often cumulated together to achieve higher calibers of security but still there is a desideratum of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

Visual cryptography is the art of encrypting information such as handwritten text, images etc. in such a way that the decryption is possible without any mathematical computations and human visual system is sufficient to decrypt the information. A secret image consists of an amassment of ebony and white pixels. Here each pixel is treated independently. For encoding the secret image, we split the pristine image into n modified versions (referred as shares) such that each pixel in a quota now subdivided into n ebony and white sub-pixels. For decoding the image, a subset S of those n shares are picked and facsimiled on separate transparencies [1].

The first form of visual cryptography is additionally kenned as secret sharing. The simplest form of visual cryptography disunites a secret image into two components so that either part by itself conveys no information. When these two components are amalgamated together by denotes of superimposition, the pristine secret can be revealed. Visual cryptography schemes were independently introduced by Shamir. Shamir divided data D into n pieces in such a way that D is facilely reconstruct able from any k pieces, but even consummate erudition of k – 1 pieces reveals absolutely no information about D. This technique sanction the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes eradicate half the pieces and security breaches expose all but one of the remaining pieces [2]. Secondly, the individuals who do not have cognizance of cryptography are indirectly getting involved in decryption. The major drawback found in this scheme is that visually blind people cannot make utilization of this technique as we perform the encryption by making the quota and person who perform the encryption those people only able to find the exact shares for performing the decryption.

a) Basic Overview on Steganography:

Steganography is the art of obnubilating the esse of the communication message afore sending it to the receiver. It has been practiced since 440 B.C. in many ways like inditing information on the back of cattle in a herd, invisible ink etc. Some relatively modern ways include obnubilating the information in newspaper articles and magazines etc. The objective of steganography is to obnubilate a secret message within a cover-media in such a way that others cannot discern the presence of the obnubilated message. Technically in simple words "steganography designates obnubilating one piece of data within another".

b) Multimedia Steganography:

It commenced in 1985 with the advent of the personal computer applied to classical steganography quandaries. Visual steganography is the most widely practiced form of steganography and is customarily done utilizing image files.

It commenced with concealing messages within the lowest bits of strepitous images or sound files. Images in sundry formats like jpeg have wide color spectrum and hence do not reflect much distortion on embedding data into them. Multimedia steganography is one of the most recent and secure forms of steganography. We shall perform steganography on image files and we shall obnubilate the encrypted message into image files in an encrypted format thus achieving a multiple cryptographic system. The most commonly used technique for image steganography is bit insertion where the LSB of a pixel can be modified. Ref [4] explicates sundry other techniques involve spread spectrum, patch work, JPEG compression etc. In lieu of traditional LSB encoding, we will utilize a modified bit encoding technique to achieve image steganography in which each pixel will store one byte of data.

c) Visual Cryptography

Visual cryptography is a cryptographic technique where visual information (Image, text, etc) gets encrypted in such a way that the decryption can be performed by the human visual system without avail of computers [1].Like other multimedia components, image is sensed by human. Pixel is the most minute unit constructing a digital image. Each pixel of a 32 bit digital color image are divided into four components, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. Human visual system acts as an OR function. Two transparent objects stacked together, engender transparent object. But transmuting any of them to non-transparent, final objects will be optically discerned non-transparent. In k-n secret sharing visual cryptography scheme an image is divided into n number of shares such that minimum k number of shares is sufficient to reconstruct the image. The division is done by Arbitrary Number engenderer [4].

2. Related Work

Proposed an authentication system for online payment utilizing both visual cryptography and Steganography which averted form identity larceny. Yet, cheating is possible which an immensely colossal drawback was. To surmount this, Tzeng [8] proposed a scheme where cheating in visual cryptography by engendering fake share can be averted by the amalgamated utilization of it with steganography. Yang et al. [5] proposed a modification to Lin proposal to avert mendacious participants from cheating. And withal this scheme incremented the quality of the stego image. According to Judge [2], the sundry steganography schemes employed in the past, present and future were discussed and their sundry forms and legitimate and illicit utilization of steganography have been discussed in brief.

a. Existing System

The subsisting system fortifies with only one type of image format only. For example, if it is .jpg, then it fortifies only that same kind of image format only. The subsisting system does not provide a cordial environment to encrypt or decrypt the data (images).The subsisting visual cryptography schemes that are utilized for data obnubilating have a security aperture in the encrypted Share file. Here an image predicated authentication utilizing Visual Cryptography is implemented.

Existing System Disadvantages:

- Does not provide a friendly environment to encrypt or decrypt the data (images).
- Supports with only one type of image format only. For example, if it is .jpg, then it supports only that same kind of image format only.
- The most critical measurements to evaluate the effectiveness of a VCS.

b. Proposed System

Proposed System, Visual Cryptography (VC), technique predicated on visual secret sharing utilized for image encryption. Secure Socket Layer (SSL) encryption obviates the interception of consumer information in transit between the consumer and the online merchant. In this paper, an incipient method is proposed, that utilizes text predicated steganography and visual cryptography, which minimizes information sharing between consumer and online merchant.VCS is a cryptographic technique that sanctions for the encryption of visual information such that decryption can be performed utilizing the human visual system. For phishing detection and obviation, we are proposing an incipient methodology to detect the phishing website. Our methodology is predicated on the Anti-Phishing Image Captcha validation scheme utilizing visual cryptography. It averts password and other confidential information from the phishing websites. Cryptographic technique :(2, 2) -Threshold VCS scheme,(n, n) -Threshold VCS scheme, (k, n) Threshold VCS scheme are utilized in this proposed system.

Advantages of Proposed System:

- Our methodology is based on the Anti-Phishing Image Captcha validation scheme using visual cryptography.
- It prevents password and other confidential information from the phishing websites.
- For phishing detection and prevention, we are proposing a new methodology to detect the phishing website.

3. Implementation

VCS utilizing cryptography is the method which uses Otsus Threshold method to engender halftone image. Where LSB matching steganography is utilized to engender embedded shares(EM).Key is utilized to engender the offset value. It converts the secret data into number of bits. Read each pixel of the cover image. If the LSB of the next cover pixel matches the next bit of secret data then do nothing else it integrates or subtract one from the cover pixel value at arbitrary. By decrypting the portions pristine shares are recuperated and stacked together to reveal secret image. To instaurate the secret, embedded shares are desteganograph with the avail of key and invert procedure is applied to reveal the secret. Performance of the system is quantified by utilizing PSNR and MSE parameters.

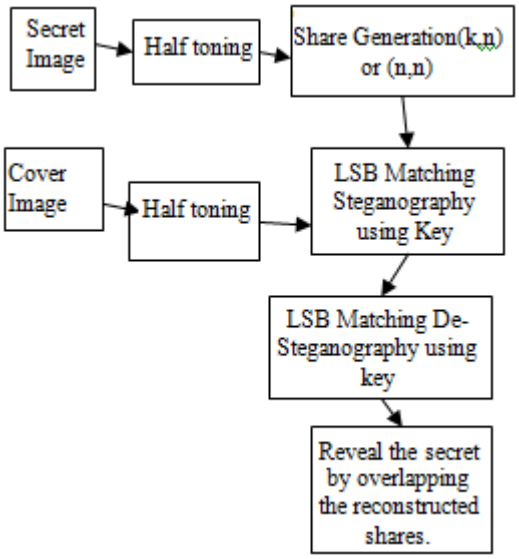

Figure 1: Proposed Method

Secret image is halftoned to engender binary image (BI).Depending on scheme the pristine shares(OS) are engendered. With the avail of key pristine shares are embedded into cover images to engender embedded shares (ES). Reconstruct shares (RS) from embedded share with the avail of same key.To reveal the secret overlap the reconstructed shares. Otsus method is utilized for halftoning and LSB.

4. Experimental Results

To evaluate the performance of proposed system we have implemented Cryptography predicated VCS utilizing Otsu's Threshold method and LSB matching steganography. LSB steganography is a puissant method to convey the secret data Images shown in Figure 3 are of type .png and of dimension 512x512 .The size of each image is different. The TEST is the secret image of type jpeg and size 2.95 KB.

Figure 2: Original Images in Database

Figure 2 shows the embedded shares of size 121KB and 123 KB respectively.

Figure 3: Embedded Shares

After Desteganography the reconstructed shares are engendered which are of same size i.e. 36.9 KB with anterior pristine shares.

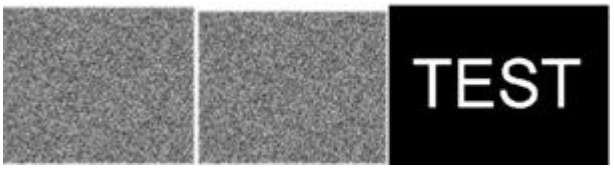

Figure 4: Reconstruct Shades Images

5. Conclusion

This paper proposed an incipient way for securing data in images while transmission utilizing the cumulation of both steganography & visual cryptography. The proposed system has discussed implementation of securely utilizing steganographic technique utilizing genetic algorithm and visual cryptography utilizing pseudorandom number. It can be concluded that when mundane image security utilizing steganographic and visual cryptographic technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganographic is highly optimized utilizing genetic algorithm. The proposed system is highly resilient against RS attack and optimally utilized for both grayscale and colored output in visual secret shares making it highly compatible for authentic-time applications.

References

[1] Feng Liu,Chuankun Wu Embedded Extended Visual Cryptographic Schemes, Vol.6,No.2 IEEE Transaction on Information Forensics ans Security, June 2011.
[2] Adi Shamir, "*How to Share a Secret,*" *in* Communications of ACM, Vol. 22, no.11, 1979, pp. 612-613.
[3] Jen-Bang Feng, Hsien-ChuWu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, "*Visual Secret Sharing For Multiple Secrets*", Pattern Recognition 41, pp.3572–3581, 2008.
[4] Wen-Pinn Fang, "*Visual Cryptography In Reversible Style*", IEEE Proceeding on the Third International Conference on intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007, Kaohsiung, Taiwan, R.O.C,2007.
[5] Pallavi V. Chavan, R.S. Mangrulkar, "*Sharing a Secret inNetwork*," in International Engineering and Technology Journalof Information System, Vol.4, no. 2, pp.83-87.
[6] Hsien-Chu Wu; Chwei-Shyong Tsai; Shu-Chuan Huang;, Colored digital watermarking technology based on visual cryptography, Nonlinear Signal and Image Processing, IEEE-Eurasip, 2005.
[7] R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001
[8] Arezoo Yadollahpour, Hossein Miar Naimi, Attack on LSBSteganography in Color and Grayscale Images Using Autocorrelation Coefficients, European Journal of Scientific Research.
[9] Andrew Ker Steganalysis of LSB matching in grayscale images, Vol.12 Issue 8IEEE Signal processing Letters, January 2005.
[10] A Text-Graphics Character CAPTCHA for Password Authentication Matthew Dailey Chanathip Namprempre

[11] [11] Jithesh, Dr. A. V. Senthil Kumar Multilayer information hiding – A blend of steganography and Visual Cryptography
[12] N. K. Ratha, J. H. Connell, R. M. Bolle Enhancing security and privacy in biometrics – based authentication systems