

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.

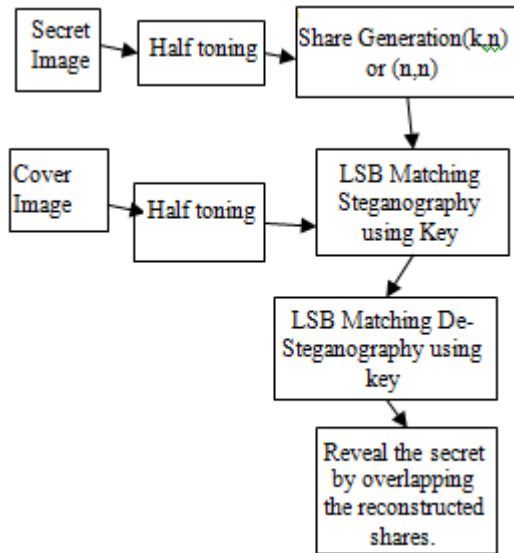


Figure 1: Proposed Method

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.

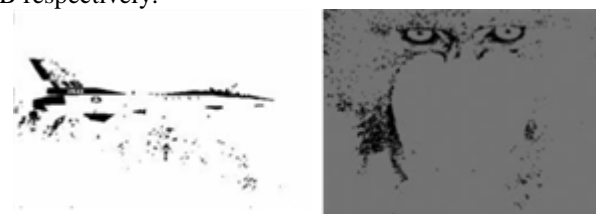


Figure 3: Embedded Shares

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

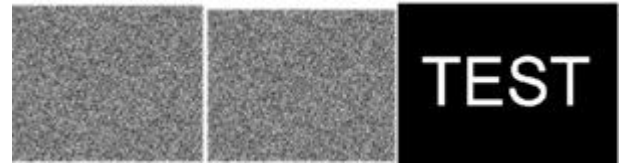


Figure 4: Reconstruct Shades Images

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 and 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-Chu Wu, 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 in Network," in International Engineering and Technology Journal of 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 LSB Steganography 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 8 IEEE 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

