ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 6, June 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Review of Various Visual Cryptography Schemes and its applications for secured communication

Ameya Parkar[1]
Assistant Prof., MCA Dept.,
Vivekanand Education Society Institute of Technology
India

Yash Mishra[2]
MCA
Vivekanand Education Society Institute of Technology
India

Abstract: ***In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when quality is not an issue, which is quite rare. The application of digital half toning techniques results in some downgrading of the original image quality due to its inherent lossy nature and it is not possible to recover the original image from its halftone version. Different types of visual cryptography schemes proposed like, VC for general access structures, for grey level images, recursive threshold, extended VC for natural images, halftone, VC for color images, Progressive, regional incrementing, segment based offers a different way to do a secure communication. Among the various schemes, RVCS enhances the embedding information efficiency by recursively hiding secret images.***

I. INTRODUCTION

Visual cryptography (VC) is a technique used for protecting image based secrets. The basic model of visual cryptography was proposed by MoniNaor and Adi Shamir in 1994 [1]. The main concept of the visual cryptography scheme is to encrypt a secret image into some shares. Secret information cannot be revealed with few shares. All shares are necessary to combine to reveal the secret image. Visual cryptography is simple, secure and effective cryptographic scheme. The operation of Visual Cryptography involves usage of two transparent images. First Image consists of random pixels and the second Image contains of the Secret Information. Both transparent images and layers are required to reveal the information. The images are encoded into multiple shares and later decoded without any Computation.

A secret is something which is kept hidden from anyone other than the intended parties [2]. Secret sharing is a process in which a secret is shared among a group of participants each one getting a piece of share. This piece of secret is known as a share. The secret can be reconstructed when all these shares are combined.

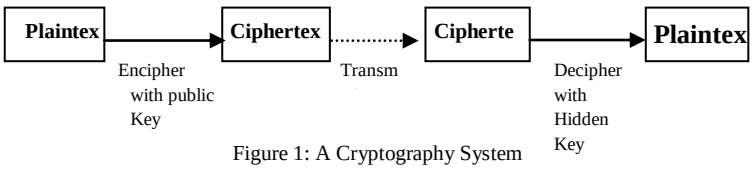

Figure 1: A Cryptography System

Let n be the no. of persons distributed the shares among themselves and k be the no. of shares within the n persons. When k shares are stacked together, the human eye does the decryption. i.e. ($k \leq n$) bring their shares, the secret can be recovered.

This further allows anyone using cryptography without its knowledge and without performing any computations. Due to these limitations this scheme is known as k-out-of-n secret sharing. The initial proceedings in the process of encryption of shares can be explained with the consideration of pixels in color coding [2] [3]. This scheme assumes the Image or a message as the combination of black and white pixels where the white pixel is transparent in colour and black pixel dark in color. When a share is received illegally by any intruders and pretends themselves as honest users [4] [5]and stacking or rearranging of the shares without proper knowledge of the share possessed by the actual person, the stacked image can turn out to be contrast and

leading to the suspicion. The shares are a collection of m black and white sub pixels arranged closely together. The structure can be considered as n x m matrix S.

II. VARIOUS VISUAL CRYPTOGRAPHY SCHEME

Following are the Different Types of Visual Cryptography Schemes which are deployed:

2.1 VISUAL CRYPTOGRAPHY FOR GENERAL ACCESS STRUCTURES

In (k, n) basic model any 'k' shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, where an access structure is a specification of all qualified and forbidden subsets of 'n' shares. Any subset of 'k' or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion.

2.2 VISUAL CRYPTOGRAPHY FOR GREY LEVEL IMAGES

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

2.3 RECURSIVE THRESHOLD VISUAL CRYPTOGRAPHY

The (k, n) visual cryptography explained in section 5.1 needs 'k' shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by AbhishekParakh and SubhashKak [4] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

2.4 EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI proposed extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, establishes the extended visual cryptography scheme suitable for natural images.

2.5 HALFTONE VISUAL CRYPTOGRAPHY

The meaningful shares generated in extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel 'P' is encoded into an array of Q1 x Q2 sub pixels, referred to as halftone cell, in each of the 'n' shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. This particular pattern maintains contrast and security.

2.6 VISUAL CRYPTOGRAPHY FOR COLOR IMAGES

The researches in visual cryptography lead to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F. Liu, C.K. Wu X.J. Lin, proposed a new approach on visual cryptography for colored images. The proposed three approaches are:

1. The first approach to realize color VCS is to print the colors in the secret image on the shares directly similar to basic model. It uses larger pixel expansion which reduces the quality of the decoded color image.

2. The second approach converts a color image into black and white images on the three color channels (red, green, blue or equivalently cyan, magenta, yellow), respectively, and then apply the black and white VCS to each of the color channels. This results in decrease of pixel expansion but reduces the quality of the image due to halftone process.

3. The third approach utilizes the binary representation of the color of a pixel and encrypts the secret image at the bit-level. This results in better quality but requires devices for decryption.

2.7 PROGRESSIVE VISUAL CRYPTOGRAPHY

In traditional Color Visual Cryptography, loss of contrast makes VCS practical only when quality is not an issue, which is quite rare. The application of digital half toning techniques results in some downgrading of the original image quality due to its inherent lossy nature and it is not possibleto recover the original image from its halftone version. Duo Jin Wei-Qi Ya n, Mohan S, Kankanhalli proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

2.8 REGIONAL INCREMENTING VISUAL CRYPTOGRAPHY

VC schemes mentioned above usually process the content of an image as a single secret i.e. all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image. The ‘n’ level RIVC scheme, an image S is designated to multiple regions associated with secret levels, and encoded to shares with the following features:

(a) Each share cannot obtain any of the secrets in S.

(b) Any t (2<t<n+1) shares can be used to reveal (t-1) levels of secrets.

(c) The number and locations of not-yet revealed secrets are unknown to users.

(d) All secrets in S can be disclosed when all of the (n+1) shares are available.

2.9 SEGMENT BASED VISUAL CRYPTOGRAPHY

The VC Methods mentioned above is based on pixels in the input image. The disadvantage of pixel based visual cryptography is loss in contrast of the reconstructed image which is directly proportional to pixel expansion ‘m’. A New approach proposed by Bernd Borchert was based on segments which takes pixels as the smallest unit to be encrypted .The advantage of segment based over pixel is that it may be easier for the human eye to recognize the symbols, The messages consists of numbers can be encoded by segment based visual cryptography using seven segment display.

III. CHEATING PREVENTION IN VISUAL CRYPTOGRAPHY

Even with the remarkable advance of computer technology, using a computer to decrypt secrets is infeasible in some situations [21][22][23]. For example, a security guard checks the badge of an employee or a secret agent recovers an urgent secret at some place where no electronic devices are available. In these situations the human visual system is one of the most

convenient and reliable tools to do checking and secret recovery. Therefore, Naor and Shamir [6] invented the visual cryptography (VC) in which a secret image (printed text, picture, etc.) is encrypted in a perfectly secure way such that the secret can be decoded directly by the human visual system.

VC is a method of encrypting a *secret image* into *shares* such that stacking a sufficient number of shares reveals the secret image[22][23][25]. Shares are usually presented in transparencies. Each participant holds a transparency (share). Unlike conventional cryptographic methods, VC needs no complicated computation for recovering the secret. The act of decryption is to stack shares and view the image that appears on the stacked shares simply. A -visual cryptography scheme [denoted as -VCS] is a visual secret sharing scheme such that stacking any or more shares reveals the secret image, but stacking fewer than shares reveals not any information about the secret image. VC has been studied intensively since the pioneer work of Noar and Shamir [1].

Most of the previous research work on VC focused on improving two parameters: *pixel expansion* and *contrast*. In these cases, all participants who hold shares are assumed to be semi-honest, that is, they will not present *false* or *fake shares* during the phase of recovering the secret image [21][23][24][25]. Thus, the image shown on the stacking of shares is considered as the *real secret image*. Nevertheless, cryptography is supposed to guarantee security even under the attack of malicious adversaries who may deviate from the scheme in any way. We have seen that it is possible to cheat in VC, though it seems hard to imagine. For cheating, a cheater presents some fake shares such that the stacking of fake and genuine shares together reveals a fake image. With the property of unconditional security, VC is suitable for sending highly classified orders to a secret agent when computing devices may not be available.

The secret agent carried some shares, each with a pre-determined order, when departing to the hostile country. When the head quarter decides to execute a specific order, it can simply send another share to the agent so that the agent can recover what the order is. We can see that it would be terrible if the dispatched share cannot be verified due to a cheater's attack. A VCS would be helpful if the shares are meaningful or identifiable to every participant. A VCS with this extended characteristic is called extended VCS (EVCS). A -EVCS is like a -VCS except that each share displays a meaningful image, which will be called *share image* hereafter. Different shares may have different share images. Atfirst glance, it seems very difficult to cheat in EVCS because the cheater does not know the share images that appear onthe genuine shares and, thus, has no information about the distributions of black and white pixels of the share images.

Based on this characteristic,they proposed a cheat-preventing method to prevent the cheater from obtaining the distribution [22][23][24]. They also proposed another cheat-preventing method in which the stacking of the genuine share and verification share reveals the verification image in some small region. We show that it is possible to attack the method.

Let us consider two types of cheaters. One is a malicious participant (MP) who is also a *legitimate participant*, namely, MP $\in$ P, and the other is a malicious outsider (MO), where MO $\notin$P. Here, we show that not only MP can cheat, but also an MO can cheat under some circumstances. A cheating process against a VCS consists of the following two phases:

1) Fake share construction phase: the cheater generates the fake shares;

2) Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In the process of cheating successfully, honest participants who present their shares for recovering the secret image may not be able to distinguish fake shares from genuine shares. A reconstructed image is *perfect black* if the sub pixels associated to a black pixel of the secret image are all black. Most proposed VC schemes have the property of perfect blackness. Since all participants together in a qualified set can recover the real secret image in perfect blackness already, it is not possible to cheat them.

IV. PERFORMANCE ANALYSIS OF VISUAL CRYPTOGRAPHY SCHEME

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [1] suggested two main parameters: pixel expansion m and contrast α. Pixel expansion m refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Jung-San Lee et al [7] advised security, pixel expansion, accuracy and computational complexity as a performance measures. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure.

Computational complexity concerns the total number of operators required both to generate the set of n shares and to restructure the original secret image C. Chang et al [5][17][23] suggested that visual cryptography scheme should support wide image format like color and gray scale. Author also argued that random looking shares appear to be suspicious and thus are vulnerable to attacks by attackers in the middle, to fill in this security gap, meaningful shares should be produced. Jen-Bang Feng et al[8] suggested that VCS should support multiple secret to work efficiently. If scheme support only one secret to share at a time to share multiple secret images numerous shares has to be generated, transmitted and maintained.

4.1 SECURITY ANALYSIS OF AUTHENTICATION OF IMAGES USING RECURSIVE VISUAL CRYPTOGRAPHY

Horng et al. proposed that cheating is possible in (k, n) VC when k is smaller than n. There are two types of cheaters in VC. One is a malicious participant (MP) who is also a legitimate participant, namely MP € P (Qualified participant) and the other is a malicious outsider (MO), where MP € P.

A cheating process against a VCS consists of the following two phases:

1. Fake share construction phase: the cheater generates the fake shares;

2. Image reconstruction phase: the fake image appears on the stacking of genuine shares and fake shares.

In order to cheat successfully, honest participants who present their shares for recovering the secret image should not be able to distinguish fake shares from genuine shares. A reconstructed image is perfect black if the sub pixels associated to a black pixel of the secret image are all black. Most proposed VC schemes have the property of perfect blackness.

For the (k, n)-threshold Visual Cryptography Scheme (VCS), a secret image is encrypted into n shared images (shares) by expanding a secret pixel into m sub pixels. Any k participants may print their shares on transparencies and stack them on the overhead projector to visually decode the secret by the human visual system. However, stacking k-1 or fewer shares will not gain any information. This distinctive property of easy decoding can be used to securely and cheaply share the printed-text secret image, e.g., the password, where no computer assistance is available or desirable. The first VCS was to encrypt the black=white secret image into noise-like shares [10][23].

Afterwards, some VCSs dealing with gray and colored images were proposed in [11]. Here the authors used the whiteness (the number of white sub pixels in a m-sub pixel block) to distinguish the black color from the white color, i.e., ‘‘- m-h’’B‘‘h’’W (resp. ‘‘m-h’’B’’h’’W) represents a white (resp. black), where h > l. For example, for a (2, 2)-VCS with h ¼ 1, l ¼ 0 and m ¼ 2, the ‘‘black’’ and the ‘‘white’’ are 2B and 1B1W (or 1W1B), respectively. And, each share contains 1B1W or 1W1B with the same frequencies so that one cannot see anything from his own share. To increase the capacity of secret images in VCS, the authors designed a recursive (2, 2)-VCS ((2, 2)-RVCS) such that the embedding efficiency of secret information is near 100% [222]. Also, their recursive method can be applied in authentication of images. In this paper we show that the secrecy of their authentication scheme is compromised. The secret information will be disclosed.

V. CONCLUSION

The RVCS enhances the embedding information efficiency by recursively hiding secret images. However, at this time, its shares are not completely random and have some related information among the sub pixels . Therefore, when applying the RVCS technology in authentication schemes, the security issue should be carefully under consideration. Due to the distinct nature of hiding, some security criteria are defined, respectively, for using the VCS and the RVCS:

(1) When one share in the (2, 2)-VCS is used as a key for authentication application, it should be shared by two parties through a secure channel. At this time, the other share can be used as a token to login;

(2) The share in (2, 2)-VCS for authentication can be used only once. The reason is that the (2,2) -VCS is just like a one-time pad. If one reuses the share, the attacker may gain some available information; and

(3) when applying (2, 2)-RVCS for authentication, except satisfying (1) and (2), all shares need to be sent through the secure channel. We have proposed three cheating methods against VCS and EVCS. We examined previous cheat-preventing schemes and found that they are either not robust enough or still improvable.

Through the process cheating prevention mechanisms an improvement on one of these cheat-preventing schemes is proposed. By our attacks, we pointed out an essential principle for a robust cheat-preventing VCS. We finally proposed an efficient transformation of VCS for cheating prevention [5]. Our transformation incurs minimum overhead on contrast and pixel expansion. It only added two sub pixels for each pixel in the image and the contrast is reduced only slightly. Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on Visual Cryptography" [7].

The proposed methodology preserves confidential information of users using 3 layers of security. 1st layer verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website, then in that situation, the phishing website can't display the image captcha for that specific user due to the fact that the image captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. Second layer cross validates image Captcha corresponding to the user. The image Captcha is readable by human users alone and not by machine users. Only human users accessing the website can read the image Captcha and ensure that the site as well as the user is permitted one or not.

So, using image Captcha technique, no machine based user can crack the password or other confidential information of the users. And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

References

1. M. Naor, and A. Shamir, (1994) "Visual Cryptography", Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950, pp. 1-12.
2. A New Visual Cryptography Scheme for Color Images B.SaiChandana.et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 1997-2000.
3. Cimato, S., R. Prisco, and A. De Santis. June 2005. ''Optimal Colored Threshold Visual Cryptography Schemes,'' Designs, Codes, and Cryptography, 35:311–335.
4. Gnanaguruparan, M. and S. Kak. January 2002. ''Recursive Hiding of Secrets in Visual Cryptography,'' Cryptologia, 26:68–76.
5. Jin, D., W. Q. Yan, and M. S. Kankanhalli. July 2005. ''Progressive Color Visual Cryptography,'' Journal of Electronic Imaging, 14:033019-1-033019-13.
6. Lin, C. C. and W. H. Tsai. January 2003. ''Visual Cryptography for Gray-level Images by Dithering Techniques,'' Pattern Recognition Letters, 24:349–358.

7. Shyu, S. J. September 2006. ‘‘Efficient Visual Secret Sharing Scheme for Color Images,’’ Pattern Recognition, 39:866–880.
8. An overview of visual cryptography Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S. International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, 2010, PP-32-37.
9. M.Naor and A. Shamir, Visual Cryptography, in “Advanced in Cryptology – EUROCRYPT‟94”, A. De. Santis, Ed., Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, PP. 1-12,1995.
10. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Visual cryptographyfor general access structures,” Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.
11. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended Schemes for Visual Cryptography, submitted to Discrete Mathematics, 1996.
12. M. Naor and B. Pinkas, “Visual authentication and identification,” in Proc. Advances in Cryptology, 1997, vol. 1294, LNCS, pp. 322–336.
13. E. R. Verheul and H. C. A. Van Tilborg, “Constructions and properties of k out of n visual secret sharing schemes,” Designs, Codes, Cryptog,,vol. 11, no. 2, pp. 179–196, 1997.
14. A Digital Image Copyright Protection Scheme Based on Visual Cryptography Tamkang Journal of Science and Engineering, Vol. 3, No. 2, pp. 97-106 (2000).
15. Randomness in secret sharing and visual cryptography schemes Annalisa De Bonis, Alfredo De Santis Theoretical Computer Science 314 (2004) 351 – 374.
16. Cheating Prevention in Visual Cryptography Chih-Ming Hu and Wen-GueyTzeng IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 1, JANUARY 2007.
17. Biehl and S.Wetzel, “Traceable visual cryptography,” in Proc. 1st Int. Conf. Information Communication Security, 1997, vol. 1334, LNCS,pp. 61–71.
18. C. Blundo and A. De Santis, “Visual cryptography schemes with perfect reconstructions of black pixels,” Comput. Graph. vol. 22, no. 4, pp. 449–455, 1998.
19. C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” J. Cryptol., vol. 12, no. 4, pp. 261–289, 1999.
20. C. Blundo, P. D’Arco, A. De Santis, and D. R. Stinson, “Contrast optimal threshold visual cryptography schemes,” SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.
21. E. F. Brickell and D. R. Stinson, “The detection of cheaters in threshold schemes,” SIAM J. Discrete Math., vol. 4, no. 4, pp. 502–510, 1991.
22. S. Cimato, A. De Santis, A. L. Ferrara, and B. Masucci, “Ideal contrast visual cryptography schemes with reversing,” Inf. Process. Lett., vol. 93, no. 4, pp. 199–206, 2005.
23. Visual Cryptography on Graphs Steve Lu, Daniel Manchala, and RafailOstrovskyAppeared in COCOON 2008: 225-234.
24. A NOVEL ANTI PHISHING FRAMEWORK BASED ON VISUAL CRYPTOGRAPHY Divya James and Mintu Philip International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012
25. Thiyagarajan, P.; Venkatesan, V.P.; Aghila, G.; "Anti-Phishing Technique using Automated
26. Challenge Response Method'", in Proceedings of IEEE- International Conference on Communications and Computational Intelligience, 2010.
27. Sun Bin.; Wen Qiaoyan.; Liang Xiaoying.; "A DNS based Anti-Phishing Approach," in
28. Proceedings of IEEE- Second International Conference on Networks Security, Wireless Communications and Trusted Computing, 2010
29. Nourian, A.; Ishtiaq, S.; Maheswaran, M.;" CASTLE: A social framework for collaborative anti-phishing databases", in Proceedings of IEEE- 5th International Conference on Collaborative
30. Computing: Networking, Applications and Worksharing, 2009.
31. Sid Stamm, ZulfikarRamzan, "Drive-By Pharming", v4861 LNCS,p495-506, 2007, Information and Communications Security - 9th International Conference, ICICS 2007, Proceedings.
32. Anthony Y. Fu, Liu Wenyin, "Detecting Phishing Web Pages with Visual Similarity Assessment
33. Based on Earth Mover’s Distance (EMD)",IEEE Transactions on Dependable and Secure Computing, v 3, n 4, p301-311, October/December 2006
34. Wenyin Liu, Xiaotie Deng, Guanglin Huang, and Anthony Y. Fu, "An Anti-phishing Strategy Based on Visual Similarity Assessment", IEEE Internet Computing, v 10, n 2, p 58-65, March/April 2006.
35. JungMin Kang, DoHoon Lee, "Advanced White List Approach for Preventing Access to Phishing Sites", 2007 International Conference on Convergence Information Technology, ICCIT 2007, p 491-496, 2007
36. Nirmal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.
37. An Extended Visual Cryptography scheme without pixel expansion for halftone images N. Askari, H.M. Heys, and C.R. Moloney 26TH ANNUAL IEEE CANADIAN CONFERENCE ON ELECTRICAL AND COMPUTER ENGINEERING YEAR 2013.

