A Review on Various Implemented Techniques for Visual Cryptography

Amit Kumar Rathore
Department of Computer Science & Engineering
Radharaman Institute of Technology & Science
Bhopal, India

Anurag Jain
Department of Computer Science & Engineering
Radharaman Institute of Technology & Science
Bhopal, India

ABSTRACT

Over the earlier period, information technology has gain access to more and more regions of our society. The expansion of digital information and telecommunication systems released a extensive collection of novel possibilities which were grab to get better the effectiveness of different sorts of procedures. The area of Visual Cryptography has progressed progressively over the past some years. It started as a procedure to encrypt binary images to hide messages containing text and has developed into encrypting color images as meaningful shares to conceal messages ranging from binary text to other color images.

Keywords

Visual Cryptography (VC), Gray Scale Images, Cryptography, Extended Visual Cryptography Scheme (EVCS).

1. INTRODUCTION

Visual Cryptography is a novel Cryptography method which is utilized to make safe the visual content such as texts or images. Visual Cryptography is an entirely protected cryptographic standard that depends on the pixel level [1], [2]. It is an instinctive, accessible technique for encrypting private data for example handwritten notes, pictures, graphical images and printed text following changing it to an image. VC exploits the human graphic scheme to decrypt the underground image from some partly covering encrypted images i.e. referred to as allocates printed on transparencies without any composite decryption algorithms or the support of computers. For this reason, it can be exploited by anyone with or without information of cryptography and without execution any cryptographic computations [3]–[4]. In Graphic Cryptography the double is separated into shares called shares which are then dispersed to the contributors. The Decryption lateral just loading the portion imageries acquires the image. The original model extended only for the second descriptions or neutral imageries. The authors change it to ensemble for the Color Images represents Gray Images and RGB/CMYK images. For the RGB/CMYK images dissimilar approaches are industrialized grounded on the color decay systems [5].

One of the approaches to keep a secret safe is secret sharing. Visual Cryptography is the distinguished method if the secret is an image. Most of the studies talk about the impress of graphic cryptography for second images. Afterward, Visual Cryptography was expanded for Gray Scale Images. Another visual cryptography method is (k, n)-threshold method. This method was explained by Naor and Shamir. In this method, a clandestine image is programmed into n shadow images also called shares. Getting better secret image involves stacking any k of the n shares but if k-1 or less stacking shares are there then no material about the clandestine image can be revealed [6].

Individual stocks in the coatings cannot reveal any useful data to attackers because these shares are random noise. If there is limited availability of share, then it is not possible to decrypt the message or information smooth with the obtainability of the computer. Randomness is the limitation of the above method and that is without any visual information. Extended form of Graphic Cryptography have been recommended which has the same disadvantages of haphazardness [7].

We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace the content with your own material.

2. THEORETICAL BACKGROUND

With the enhancement in digital media they require for methods to keep such information is flattering more essential. The cause of digital media's expansion can be associational to the assets of information provided by the Internet. The quantity of information that is downloaded and uploaded enlarges each day with information ranging from straightforward text documents to photos of objects to hyper-spectral double dices of the biosphere. The Internet delivers a no difficulty of access that necessitates material of the most excellent method to protect the visual information obtainable on the Internet from stealing, duplication or unauthorized employ.

The area of Graphic Cryptography has been enlarged over the previous numerous years. The unique technique was proposed by Naor and Shamir [9] for binary images. This makes available a completely protected scheme where secret letters are controlled in “shares". Separately these shares are similar to random noise but when they are stacked and supported completely their message is decrypted using only the human visual scheme. While this technique presents safety measures for text and binary images the expansion of digital media needs the expansion of this technique to provide security for gray and color images. Numerous techniques have been expanded for safeguarding gray and tint images including half-toning, dithering, color sub pixel groupings and significant image shares [8, 10]. All the way through this development of the unique technique Visual Cryptography make available a secure method to accumulate and broadcast text, binary images, gray images and color images. In view of the fact that the unique method was make public in 1994 there have been a great quantity of differences, alterations and developments additional to the compilation of obtainable Visual Cryptography methods. As the numeral of published techniques enhance a method for estimate the efficiency, excellence and perfect employ of each of the algorithms is essential. At present, this data can be established by reading all the way through the paper, estimating its substances, and influential if it is an appropriate technique for a given project. While it is achievable to complete this procedure on numerous algorithms before deciding on the ultimate technique to be utilized it would be valuable for a set of normal and presentation metrics to be obtainable for utilize in shaping the perfect Visual Cryptography technique for a particular project. The growth of an appropriate standard method would permit these usual and presentation metrics to subsist in one identical format. The substances of this standard method would contain information observing the competence of the algorithms. It would establish the most significant move toward and methodology utilized to produce the image shares. In addition, it would make available external accomplishment and confirmation of the code accessible to accomplish the algorithm. In addition, it would make available information on image reform in general feature of reconstructed images and a ranking (or grade) of the algorithm evaluated to a given Visual Cryptography average.

3. VISUAL CRYPTOGRAPHY

Visual Cryptography is a unique type of cryptography which encrypts graphic material i.e., printed text, handwritten notes, images, etc. into n see-through images distributes so that human beings can achieve the decryption visually without the help of computers [11]. Each one of n transparent images is an impossible to differentiate from random noise consequently they can be broadcast or shared over an insecure communication channel i.e., Internet. Consequently for the reason that the splits become visible as indiscriminate binary models the assailants cannot intellect any suggestions about a top clandestine duplicate from individual distributes [12]. The top secret material can be decrypted from the splits in a conventional line by the hominid visual organization when all or any preponderance of the divides are stacked mutually so that the sub-pixels are suspiciously supported. Conversely, any minority number of stacked splits or every share independently cannot reveal any suggestion about the secret data even if computers are accessible [13]. The essential representation of visual cryptography concentrate on by Naor and Shamir, splits every pixel in an new image into 2×2 black and white sub-pixels in the two splits by reason of the rules in Table 1. As in Table 1, a white pixel is encrypted into two identical blocks in the two shares and a black pixel is encrypted into two corresponding blocks in the two shares. Each block is 2×2 black and white subpixels. Take Fig. 2 for example. It gives you an idea about the result obtained according to Table 1. The innovative underground duplicate (a) is coded into two translucent shares (b) and (c). We can become the improved underground image (d) when these two see-through dividends (b) and (c) are superimposed mutually and with awareness supported.

Table 1: Naor and Shamir's (2, 2) visual cryptography arrangement of black and white pixels (adapted from [12])

Pixel of the secret image	□ White pixel		■ Black pixel	
Share 1	■□ □■	□■ ■□	■□ □■	□■ ■□
Share 2	■□ □■	□■ ■□	□■ ■□	■□ □■
Stacked results (Share 1+ Share 2)	■□ □■	□■ ■□	■■ ■■	■■ ■■

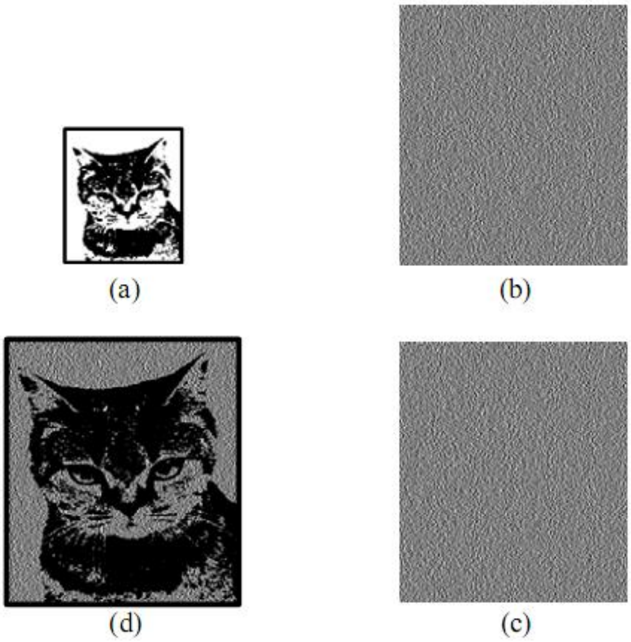
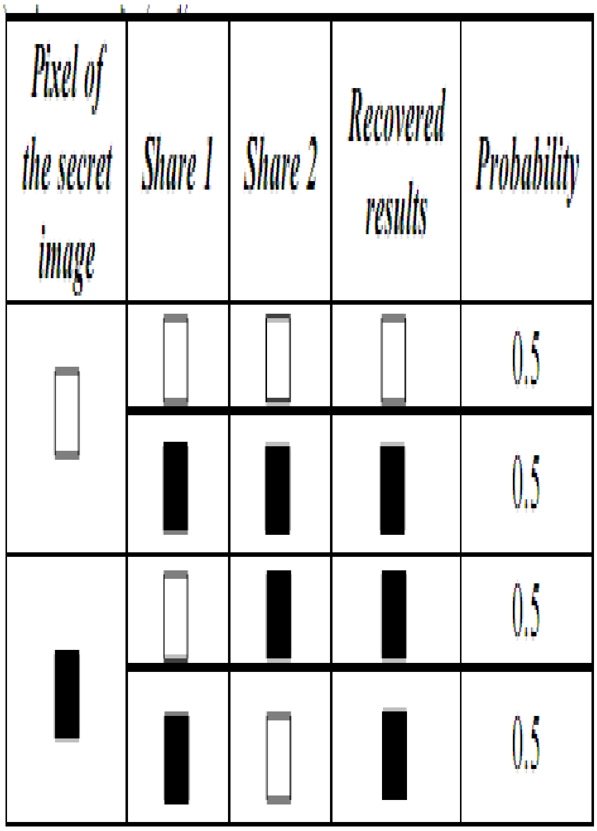


Fig. 2 The imprint of Naor and Shamir's (2, 2) graphic cryptography method with four subpixels: (a) The unique clandestine image, (b) The first share, (c) The second share, (d) The recovered image by superimposing (b) and (c).

Most studies of visual cryptography systems are based on the method of pixel expansion; consequently, the consequential allocates of encrypted secret image by this method are enlarged numerous times of the original dimension by this means causing many difficulties for ex., image distortion utilize of more memory space and complexity in taking splits. To defeat the above revealed difficulties, Ito et al. [14] and Yang [15] planned non-expansion graphic cryptography or so called probabilistic graphic cryptography (ProbVC) model for black and white images explicitly they joined the conservative visual cryptography with the idea of the possibility and without pixel expansion. In their representations the dimensions of the original image divides i.e. shadow images and the make progressed image are the similar. Each pixel in the innovative underground image is stand for as a black or white pixel in the splits and the new top clandestine image can be differentiated by superimposing these shares together.

ProbVC models in a straight line utilize the convenient two n×n Boolean basis matrices S^0 and S^1 to produce the splits. To encode a pixel from the clandestine image in ProbVC models one indiscriminately chooses a column in S^0 or S^1 rendering to the color of the pixel i .e. white or black and allocates i-th row of the selected column to i-th share i.e. equivalent share. Ito et al. [14] defined a novel limitation $\beta=|p_0-p_1|$ to stand for the difference of the make progressed image, where p_0 and $p_1$are the probabilities with which a black pixel on the improved image is generated from a white and black pixel on the clandestine image correspondingly. Table 2 give you an idea about Ito et al.'s (2, 2) ProbVC method that a pixel on a black and white clandestine copy is mapped into a matching pixel in each of the two shares i.e. without pixel expansion. The clandestine image is make progressed by stacking and supporting watchfully the pixels of the two splits where every pixel in share 1 is superimposed on the equivalent pixel in share 2; this is achieved through the OR operation on the two transparent shares [16]. Fig 3 demonstrates the result acquired according to Table 2. In the following part, ProbVC models will be utilized to build our proposed public-key encryption method.

Table 2: Ito et al.'s (2, 2) ProbVC method of black and white pixels (personalized from [14, 16])



Pixel of the secret image	Share 1	Share 2	Recovered results	Probability
□	□	□	□	0.5
	■	■	■	0.5
■	□	■	■	0.5
	■	□	■	0.5

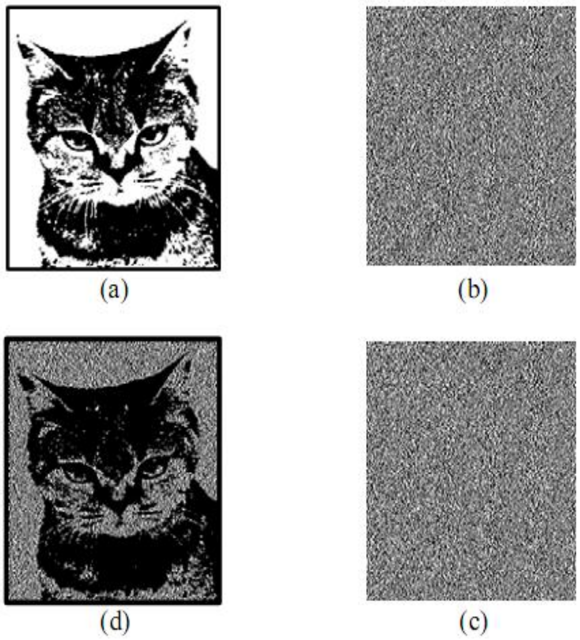


Fig. 3 An example of (2, 2) ProbVC method without pixel development: (a) The unique underground image, (b) The first share, (c) The second share, (d) The recovered image by superimposing (b) and (c)

4. EXISTING VISUAL CRYPTOGRAPHY METHODS

Visual Cryptography for Gray Level Images: earlier attempts in visual cryptography were confidential to binary images which is inadequate in authentic time applications. Chang-Chou Lin, Wen-HsiangTsai [17] planned visual cryptography for steely level imageries by dithering methods. As an alternative of using gray sub pixels in a straight line to created splits, a dithering method is utilized to alter gray level images into estimated binary images. Then offered graphic cryptography approaches for second images are useful to achieve the work of creating splits. The result of this method is at rest acceptable in the features of enlarge in comparative size and decoded image quality even when the number of gray levels in the original image unmoving reaches 256.

Visual Cryptography For common Access Frameworks: In (k,n) Basic model any "k" shares will decode the clandestine image which decreases safety measures stage. To defeat this problem the fundamental representation is expanded to common right to use arrangements by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson[18],where an access arrangement is a condition of all capable and prohibited subsets of "n" shares . Any subset of "k" or more competent shares can decrypt the underground image but no data can be acquired by stacking lesser number of experienced shares or by stacking prohibited shares. Structure of this idea is unmoving suitable in the features of enlarge in comparative size and decoded image quality even when the amount of gray levels in the original image unmoving reaches 256.

Recursive Threshold Visual Cryptography: The (k,n) visual cryptography give explanation in section I needs "k" shares to rebuild the underground image. Each share consists at most [1/k] bits of secrets. This move toward experiences from inadequacy in conditions of number of bits of secret expressed per bit of shares. Recursive threshold visual cryptography planned by Abhishek Parakh and SubhasKak

[19] eradicates this difficulty by thrashing of smaller secrets in shares of larger secrets with secret sizes repetition at every step. When Recursive threshold visual cryptography is utilized in network application network load is decreased.

Halftone Visual Cryptography: The significant splits produced in Protracted graphic cryptography planned by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [20] was of poor feature which again enhances the doubt of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo planned halftone visual cryptography which amplifies the feature of the significant shares. In halftone painterly cryptography a undisclosed second pixel "P" is determined into an display of Q1 x Q2 ("m" in indispensable prototypical) sub pixels documentation on to as halftone cell, in each of the "n" shares. By use halftone cells with a suitable size visually pleasing halftone shares can be acquired. Also sustains difference and security.

Extended Graphic Cryptography for Natural Images: All of the Graphic Cryptography techniques undergo from a rigorous constraint which delays the ideas of Visual Cryptography. The drawback be positioned in the fact that all shares are inherently random patterns carrying no visual information, increasing the feeling of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI [20] anticipated Protracted painterly cryptography for accepted pictures theories substantial second images as dividends. This determination decreases the cryptanalysts to estimate coverts from a human being shares. While the preceding examines fundamentally switch only double images, [20] establishes the lengthy graphic cryptography scheme suitable for natural images.

Progressive Visual Cryptography: In conventional Color Visual Cryptography loss of distinction makes VCS practical only when superiority is not an subject, which is quite rare. The application of digital half toning methods consequences in some downgrading of the innovative image quality due to its inherently lossy nature and it is not feasible to get better the unique image from its halftone description Duo Jin Wei-Qi Yan, Mohan S, Kankanhalli [21] wished-for a novel encoding system that allows us to change gray-scale and hue images into colorless ones exclusive of loss of any data. Incorporate this novel encoding system into visual cryptography method permits ideal improvement of the secret grayscale or color image.

Visual cryptography for Color Images: The researches in visual cryptography guides to the dreadful conditions in the feature of the decoded binary images which formulates it inappropriate for security of color image. F.Liu,C.K. Wu X.J. Lin proposed a novel method on visual cryptography for colored images. They proposed three methods as follows:

- The initial method to understand color VCS is to print the colors in the secret image on the splits in a straight line comparable to essential representation. It exploits better pixel expansion which decreases the excellence of the decoded color image.
- The subsequent approach translates a color image into black and white images on the three color channels i.e. red, green, blue or consistently cyan, magenta, yellow, correspondingly and then affect the black and white VCS to each of the color channels. This effects in reduce of pixel development but shrinks the feature of the image appropriate to halftone procedure.
- Another approach develops the binary illustration of the color of a pixel and encrypts the secret image at the bit-level. This effects in enhanced feature but needs piece of equipments for decryption.

Regional Incrementing Visual Cryptography: Visual Cryptography methods declared above more often than not procedure the substance of an image as a single secret i.e. all of the pixels in the clandestine twin are split using a single encoding rule. This kind of sharing rule make known moreover the complete image or not anything and for this reason boundary the secrets in an image to have the equivalent confidentiality assets. Ran-Zan Wang [22] proposed Region Incrementing Visual cryptography for sharing visual top secrets in various confidentiality heights in a distinct image. The "n" level RIVC method an image S is assigned to various areas combined with top secret stages and predetermined to divides with the following characteristics:

- Each share cannot acquire any of the top secrets in S,
- Any t(2<t<n+1) shares can be utilized to make known (t-1) stages of secrets
- The amount and positions of not up till now exposed top secrets are unidentified to clients,
- All top secrets in S can be revealed when all of the (n+1) shares are accessible,

Segment Based Visual Cryptography: The Visual Cryptography schemes revealed on top of is based on pixels in the input image. The drawback of pixel based visual cryptography is beating in contrast of the reconstructed image which is in a straight line comparative to pixel expansion "m". A novel method anticipated by Bernd Borchert [18] was based on subdivisions which acquires pixels as the smallest unit to be encrypted. The benefit of segment supported over pixel is that it may perhaps be easier for the human eye to distinguish the representations. The mails contains of statistics can be prearranged by subdivision based visual cryptography using seven segment display.

5. LITERATURE SURVEY

In this paper [24], here author have clarified the novel COALA organization for graphic picture of the cryptographic procedures, and experiences from using it at the Data Security course taught at the SEE-UB. The software system is designed to support the laboratory exercises which cover complex cryptography algorithms like: DES, AES, RSA and Diffie-Hellman that are taught in the course. To the greatest of our information this is the initial application of the AES algorithm in a learning supporting tool. Also, unlike other existing tools which describe other mentioned algorithms, COALA has the possibility to walk students through the whole algorithm execution step-by-step using real world examples. The functional description of the system and several key design and implementation details are presented in the paper.

The most important objective of the beginning of the COALA system in the Data Security course was to help students to better recognize the algorithms taught in the course and to help them prepare for the exam. Numerical indicators show [24] that the percentage of the students who accepted the exam and the standard grade on the assessments for the duration of one school year increased for the students who used the COALA system. Results of measurements showed that the introduction of the COALA system brought benefit to all students, especially to those students who previously could not pass the exam in the first examination period of a school year and to some of the best students to improve their grades.

In [23], A Visual cryptography method permits visual material i.e. movies, manuscript, etc. to be encrypted in such a method that decryption develop into such a motorized process for which there is no requirement of a computer. There is splitting of original image into shares and it can't be possible for unauthorized person to get the data which is hidden within that share images. The secret data can be revealed just by stacking the two shares.

Hundhausen et al. in [25] explained algorithm visualization effectiveness. Four underlying theories were defined: Epistemic Fidelity, Dual-coding, entity differences and Cognitive Constructivism. It was stated that the Cognitive Constructivism theory has had the most significant impact on AV efficiency out of these four. According to this philosophy scholars will not benefit from an AV system by passively viewing the algorithm simulation, but instead they must become actively engaged with the technology in order to advantage most from it. The second conclusion that is important is the way in which the consequences of an AV scheme can be calculated. There are two significant features that collision dimension of an AV scheme efficiency: the category of information that is determined i.e. theoretical information and/or technical information and the method facts acquirement is calculated i.e. post-test results dimension and/or pre-test to post-test development amount.

It was accentuated that using dynamic learning methods enhances students motivation and holds their attention longer than lecturing alone [26]. Some topics covered in security sequences can be very stimulating to scholars i.e. viruses, hackers, etc., in distinction to the issues ideas and assumption on which they are based on e.g., algorithms which are typically less attractive and more challenging to students. Schweitzer et al. in [26] suggested that these less attractive topics should be covered by dynamic learning methods to facilitate maintain student's interest. Although there are a lot of visualization tools that are used in the teaching development, there are a relatively low number of these tools that are used in security education and particularly for cryptographic procedures. We analyzed the likelihood to use above-mentioned obtainable tackles and their appropriateness for the Information Security course.

A visualization device for wireless system attacks is accessible in [27]. Approximately of the most predominant wireless system attacks i.e. snooping, evil identical, man in the mid, ARP murdering, and ARP request repetition have been confirmed with this tool. Demonstrations are in the form of animations and options that are available to users during an animation are: play draw gradually reverse to distinguish the preceding pace further to observe the next step, break in proceedings and discontinue. The tool gives a quiz that clients can take with queries on the animation they immediately ended.

In [28] a set of communicating picturing applets for instruction cryptography procedures is available. Algorithms enclosed by this tool are: Shift Cipher, easy Substitution Cipher, Affine Cipher, RSA Cipher, Vigenere Cipher, RC4 Stream Cipher, and DES Cipher. The boundary permits clients to contribution the text to be encoded and the explanation and to interactively achieve examination tools such as key length analysis, frequency graphs and diagram maps. The applet for DES Cryptograph give you an idea about two rounds of a Feistel system as a illustration with textual explanation of operations in a encompassing and it interactively moves bits through the diagram to illustrate data flow in the algorithm.

Grasp [29] is a imagining tool for education safety protocols. It can be arranged by a user to visualize any security protocol (e.g., Diffie-Hellman), since it provides procedure requirement linguistic that permits a random quantity of performers and communication passing with suitable commands needed for security protocols. Users can edit protocol commands during the visualization permitting them to scrutinize "what-if" scenarios and they can control the protocol execution by moving a step forward or backward, resetting or finishing the execution.

In [7], case of color graphic cryptography methods, there is no limitation of randomness on color images. Error dispersion and pixel harmonization are the two basic methods used. One of the simple method is Error diffusion in which the there is filtering of quantization mistake at each pixel equal and is further fed as the input to the next pixel. In this way, low frequency gotten among the contribution and production image is diminished which consequences in superiority images. Color degradation is circumvented with the assistance of pixel organization. An well-organized hue image pictorial cryptic sieving arrangement has been presented by this proposal for improving the double superiority on reinstated unique image from pictorial mysterious shares. A consequence called De-blurring consequence is accessible by the recommended color image pictorial mysterious filtering method on the non-uniform distribution of visual cryptic distributes pixels. After the removal of blurring effects on the pixels there is require to be appropriate Fourier transformation to standardize the randomly altered share pixels on the unique restored image. As an effect, the quality of restored visual cryptographic image is developed to its optimal point.

6. CONCLUSION

In this newspaper we have review on various existing visual cryptography methods for pictorial representation of the cryptographic algorithms. Here in this weekly we try to associates the double superiority and security using a variety of visual cryptography methods. All together security is also an important issue. Hence investigation in pictorial cryptography (VC) is concerning upholding the dissimilarity at the identical time preserving the refuge.

7. REFERENCES

[1] J. Pejaś, M. Zawalich, "Visual Cryptography Methods as a Source of Trustworthiness for the Signature Creation and Verification Systems," Advances in Information Processing and Protection, Springer, USA, 2008, pp. 225–239.

[2] I. Fischer and T. Herfet, "Watermarks and Text Transformations in Visual Document Authentication," Journal of Computers, vol. 2, no. 5, pp. 44–53, 2007.

[3] K. Manglem, S. Nandi, S. Birendra, L. Shyamsundar, "Stealth Steganography in Visual Cryptography for Half Tone Images," in Proc. of the International Conference on Computer and Communication Engineering, Malaysia, 2008.

[4] Y. C. Hou, S. F. Tu, "A Visual Cryptographic Technique for Chromatic Images Using Multi-pixel Encoding Method," Journal of Research and Practice in Information Technology, vol.37, no.2, pp. 179–192, 2005.

[5] Sankar Das, Sandipan Chowdhury and Dibya Chakraborty, “Visual Cryptography using Three Independent Shares in Color Images”, International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Issue 4, Volume 2 (April 2015).

[6] Kun-Yuan Chao*, Ja-Chen Lin,”(2, 3)-threshold visual cryptography for color images”, Proc. Of the 6th WSEAS Int. Conf. On Signal Processing, Computational Geometry & Artificial Vision, Elounda, Greece, August 21-23, 2006 pp. 89-94.

[7] Shiny Malar F.R, Jeya Kumar M.K,” Error Filtering Schemes for Color Images in Visual Cryptography”, International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, 2011.

[8] Der-Chyuan Lou, Hong-Hao Chen, Hsien-Chu Wu, and Chwei-Shyong Tsai. A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares. Displays, 32:118-134, February 2011.

[9] Moni Naor and Adi Shamir. Visual cryptography. EUROCRYPT, pages 1-12, 1994.

[10] C-C Chang, W-L Tai, and C-C Lin. Hiding a secret colour image in two colour images. The Imaging Science Journal, 53:229-240, May 2005.

[11] A. D. Bonis, and A. D. Santis, "Secret Sharing and Visual Cryptography Schemes", Proceedings of the IFIP TC11 16th International Conference on Information Security, (2001), pp. 123-138.

[12] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition, Vol. 36, No. 7, (2003), pp. 1619-1629.

[13] R. Youmaran, A. Adler, and A. Miri, "An Improved Visual Cryptography Scheme for Secret Hiding", 23rd Biennial Symposium on Communications, (2006), pp. 340-343.

[14] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography", IEICE Trans. Fund., Vol. E82-A, No.10, (1999), pp. 2172-2177.

[15] C.-N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognition Letter, Vol. 25, No. 4, (2004), pp.481-494.

[16] S.-F. Tu, "On the design of protection scheme for digital images and documents based on visual secret sharing and Steganography", Ph.D. Dissertation, Department of Information Management, National Central University, Taiwan, (2004).

[17] Zhou, G. R. Arce, and G. Di Crescenzo, “Halftone Visual Cryptography,” IEEE transactions on Image Processing, to appear in 2006.

[18] M. Naor and B. Pinkas, “Visual authentication and identification,” Crypto97, LNCS, vol. 1294, pp. 322–340, 1997.

[19] M. Naor and A. Shamir, “Visual Cryptography,” in Proceedings of Euro crypt 1994, lecture notes in Computer Science, 1994, vol. 950, pp. 1–12.

[20] A. Bonnis and A. Santis, “Randomness in secret sharing and visual cryptography schemes,” Theory. Computer Science, 314, pp 351- 374 (2004).

[21] E. Myodo, S. Sakazawa, Andy. Takishima, “Visual cryptography based on void-and-cluster half toning technique,” in Proc. IEEE ICIP, Atlanta, GA, Oct. 2006.

[22] R. Hwang, “A digital Image Copyright Protection Scheme Based on Visual Cryptography,” Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).

[23] Jainthi.k, Prabhu.P ,”A novel cryptographic technique that emphasis visual quality and efficieny by floyd steinberg error diffusion method”, International Journal of Research in Engineering and Technology, eISSN: 2319-1163 pISSN: 2321-7308,Volume: 04, Issue: 02 Feb-2015.

[24] Zarko Stanisavljevic, Jelena Stanisavljevic, Pavle Vuletic, and Zoran Jovanovic, “COALA-System for Visual Representation of Cryptography Algorithms” IEEE Transactions On Learning Technologies, Vol. 7, No. 2, April-June 2014.

[25] C. D. Hundhausen, S. A. Douglas, and J. T. Stasko, “A meta-study of algorithm visualization effectiveness,” J. Vis. Languages Comput., vol. 13, no. 3, pp. 259–290, Jun. 2002.

[26] D. Schweitzer, D. Gibson, and M. Collins, “Active learning in the security classroom,” in Proc. IEEE 42nd Hawaii Int. Conf. Syst. Sci., Jan. 2009, pp. 1–8.

[27] X. Yuan, R. Archer, J. Xu, and H. Yu, “A visualization tool for wireless network attacks,” J. Educ., Inf. Cybern., vol. 1, no. 3, pp. 53–58, 2009.

[28] D. Schweitzer and L. Baird, “The design and use of interactive visualization applets for teaching ciphers,” in Proc. IEEE Inf. Assurance Workshop, Jun. 2006, pp. 69–75.

[29] D. Schweitzer, L. Baird, M. Collins, W. Brown, and M. Sherman, “GRASP: A visualization tool for teaching security protocols,” in Proc. 10th Colloquium Inf. Syst. Security Educ., Jun. 2006, pp. 75–81.