ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

The algorithm of (t, ∞) OptPrVC scheme Implementation within Dynamic Group for Secure Data Access

Mr.Tatarao Moka
M.Tech Student,
Department of CSE,
Srinivasa Institute of Engineering and Technology,
Cheyyeru (V), Amalapuram.

Mr. S N V S S S T Murty
Associate Professor,
Department of CSE,
Srinivasa Institute of Engineering and Technology,
Cheyyeru (V), Amalapuram.

Abstract:

Phishing is one of the attacks that became popular recently. It is a duplicate copy of web page used to acquire personal and confidential information of user like credit card details by legitimate entity in an electronic communication. In this project we have proposing a new technique named as "New Probabilistic Model Of (t, ∞) VC Scheme" to solve the problem of phishing Visual cryptography is to encrypt a secret image into some shares (transparencies) such that any qualified subset of the shares can recover the secret visually. The (t, ∞) is VC scheme required t number of shares (transparencies) out of n number of shares (transparencies). Here original image is divided into n number of shares, where one share stores with user and the remaining shares store in server. User's share is stacked with servers share to reveal the secret image for identifying phishing website; the individual sheet images do not reveal the secret image. The decryption is possible only when commerce bank can provide both shared at a time. In this project we used (t, ∞) VC Scheme based on basis matrices and the probabilistic model.

Key words:

Probabilistic scheme, Contrast, random grids (RGs), secret sharing, visual cryptography (VC).

1 INTRODUCITON:

Visual Cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into transparencies and the content of each transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques.

In general, a -threshold VC scheme has the following properties: The stacking of any out of those VC generated transparencies can reveal the secret by visual perception,but the stacking of any or fewer number of transparencies cannot retrieve any information other than the size of the secret image.

Another important metric is the pixel expansion denoting the number of subpixels in transparency used to encode a secret pixel. The minimization of pixel expansions has been investigated in previous studies.

The probabilistic model of the VC scheme was first introduced by Ito, where the scheme is based on the basis matrices, but only one column of the matrices is chosen to encode a binary secret pixel, rather than the traditional VC scheme utilizing the whole basis matrices. The size of the generated transparencies is identical to the secret image.

In this paper, we obtain improved in approximability results for three problems, viz. the problem of finding the size of the largest clique in a graph, finding the chromatic number of a graph, and approximate coloring of a graph, the graph is guaranteed to have a small constant chromatic number.

The first two results are obtained via new PCP constructions based on Hadamard codes while the third result is derived from a simple new reduction. From a conceptual point of view, the result on approximate graph coloring is the most interesting.

The first step towards proving strong in approximability result for Max Clique was taken in the seminal paper by Feige which showed a connection between Probabilistically Checkable Proof Systems and in approximability of Max Clique.

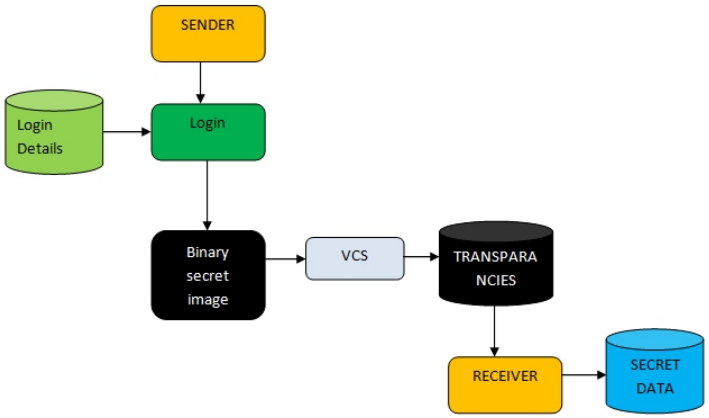
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

1.1 Survey of Visual Cryptography Schemes:

Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images(either binary or color) and number of secret images(either single or multiple) encrypted by the scheme. Intent of this paper is on study and performance analysis of the visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated.

2.ARCHITECTURE:

Login or logon (also called logging in or on and signing in or on) is the process by which individual access to a computer system is controlled by identification of the user using credentials provided by the user. A user can log in to a system to vyfvs and can then log out or log off (perform a logout / logoff) when the access is no longer needed. Logging out may be done explicitly by the user performing some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by powering the machine off, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period. After logging in, in this module we design to take the input image for processing.



2.1 EXISTING SYSTEM:

» Generally, the stacking revelation of the secret with higher contrast represents the better visual quality, and therefore the stacking secret with high contrast is the goal of pursuit in VC designs.]

» Based on the definition of contrast, there are studies attempting to achieve the contrast bound of VC scheme.

» Blundo et al are given the optimal contrast of VC schemes.Hofmeister et al. provide a linear program which is able to compute exactly the optimal contrast forVC schemes.

» Moreover, there exist VC related researches using differential definitions of contrast.

» Another important metric is the pixel expansion denoting the number of sub pixels in transparency used to encode a secret pixel.

» The minimization of pixel expansions has been investigated in previous studies. where the scheme is based on the basis matrices, but only one column of the matrices is chosen to encode a binary secret pixel, rather than the traditional VC scheme utilizing the whole basis matrices.

Disadvantages:

» Here the scheme is based on only one column of the matrices is chosen to encode a binary secret pixel, rather than the traditional VC scheme utilizing the whole basis matrices.

» Does not use Transparencies is unable to extract any information about the secret.

» Less security can provide the upper bound and lower bound of the optimal contrast for VC schemes.

2.2PROPOSED SYSTEM:

» Proposed a probabilistic model of VC scheme, and the two cases and are explicitly constructed to achieve the optimal contrast. Based on Yang [31], Cimato et al.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

» Proposed a generalized VC scheme in which the pixel expansion is between the probabilistic model of VC scheme and the traditional VC scheme.

» The visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into transparencies, and the stacking of any out of transparencies reveals the secret image.

» paper proposes a VC scheme with unlimited based on the probabilistic model. The proposed scheme allows to change dynamically in order to include new transparencies without regenerating and redistributing the original transparencies.

» Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed.

» An equation is derived from the fundamental definitions of the VC scheme, and then the VC scheme achieving maximal contrast can be designed by using the derived equation.

» The maximal contrasts with to are explicitly solved in this paper.

Advantages:

» The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices.

» The number of generated transparencies of a VC scheme.

» It's highly secured. Unlimited based on the probabilistic model.

» VC scheme, and then the VC scheme achieving maximal contrast can be designed by using the derived equation.

3.PROCESS DIAGRAM

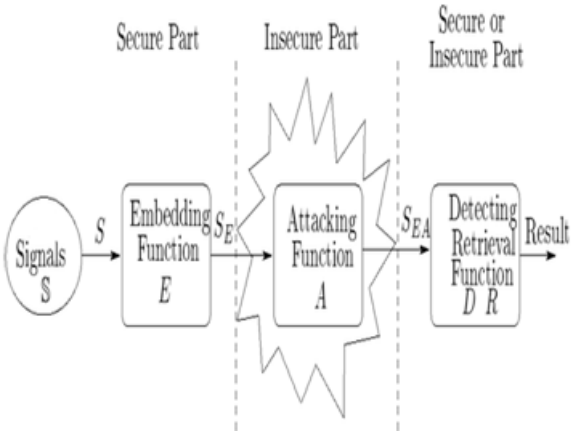


Fig: Process Diagram

3.1Visual cryptography Implementation:

This module is the core for the project, where we implement the Visual Cryptography. We used (t, n) Visual cryptography algorithm. The (t, n) Visual cryptography algorithm is applied for the gray scale image here. As a pre-processing step, a dictionary is prepared for the gray scale image. In this dictionary, the string replaces characters with single quotes. Calculations are done using dynamic Huffman coding. In compression of grey scale image select the information pixels. Then generate halftone shares using error diffusion method. At last filter process is applied for the output gray scale images. Filters are used to improve the quality of reconstructed image to minimize the noises for sharpening the input secret image.

3.2 Encoding:

A dictionary is initialized to contain the single-character strings corresponding to all the possible input characters (and nothing else except the clear and stop codes if they're being used). The algorithm works by scanning through the input string for successively longer substrings until it finds one that is not in the dictionary. When such a string is found, the index for the string less the last character (i.e., the longest substring that is in the dictionary) is retrieved from the dictionary and sent to output, and the new string (including the last character) is added to the dictionary with the next available code. The last input character is then used as the next starting point to scan for substrings.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

3.3 Decoding:

The decoding algorithm works by reading a value from the encoded input and outputting the corresponding string from the initialized dictionary. At the same time it obtains the next value from the input, and adds to the dictionary the concatenation of the string just output and the first character of the string obtained by decoding the next input value. The decoder then proceeds to the next input value (which was already read in as the "next value" in the previous pass) and repeats the process until there is no more input, at which point the final input value is decoded without any more additions to the dictionary.

In this way the decoder builds up a dictionary which is identical to that used by the encoder, and uses it to decode subsequent input values. Thus the full dictionary does not need be sent with the encoded data; just the initial dictionary containing the single-character strings is sufficient (and is typically defined beforehand within the encoder and decoder rather than being explicitly sent with the encoded data.)

3.4 Login modules:

Login or logon (also called logging in or on and signing in or on) is the process by which individual access to a computer system is controlled by identification of the user using credentials provided by the user.

A user can log in to a system tovyfvs and can then log out or log off (perform a logout / logoff) when the access is no longer needed.Logging out may be done explicitly by the user performing some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by powering the machine off, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.

3.5 Matrices (Black and White) Method:

The basis matrices of VC scheme were first introduced, a white-and-black secret image or pixel is also described as a binary image or pixel. In the basis matrices, to encode a binary secret image, each secret pixel white black will be turned into blocks at the corresponding position of transparencies, respectively. Each block consists of subpixels and each subpixel is opaque or transparent. Throughout this paper, we use 0 to indicate a transparent subpixel and 1 to indicate an opaque subpixel. If any two subpixels are stacked with matching positions, the representation of a stacked pixel may be transparent, when the two corresponding pixels are both transparent.

3. 6 Scheme Method:

Proposed method is based on the basis matrices and the idea of probabilistic model. For a (t, n) VC scheme, the "totally symmetric" form of (B0)and(B1) are both constructed and described as H0 and H1, respectively. VC scheme with flexible value of (n). From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group.

3.7 Encoding Algorithm Method:

For a given value of (t), the transparencies can be continuously generated with the OptPrVC scheme. However, practical applications require the algorithm to terminate within finite steps. To meet the requirement, a finite number is used to specify the number of transparencies in the algorithm.

4.CONCLUSION:

We propose a practical cloud storage system called FADE, which aims to provide access control assured deletion for files that are hosted by today's cloud storage services. We associate files with file access policies that control how files can be accessed. We then present policy-based file assured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked. We describe the essential operations on cryptographic keys so as to achieve access control and assured deletion. FADE also leverages existing cryptographic techniques, including attribute-based encryption (ABE) and a quorumof key managers based on threshold secret sharing.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

We implement a prototype of FADE to demonstrate its practicality, and empirically study its performance overhead when it works with Amazon S3. Our experimental results provide insights into the performance-security trade-off when FADE is deployed in practice.

In this paper we proposed Virtual cryptography scheme with n values. From the experimental perspective, the proposed one accommodates the dynamic changes of users without regenerating and redistributing the transparencies in here , in which it reduces computation and communication resources required in managing the dynamically changing the user's group.

With the theoretical experiments perspective, this scheme can be considered as the prospect mold of VC with unlimited n. Initially, the proposed scheme is based on basis matrices of experiment, but here the basis matrices with infinite size cannot be constructed practically. Therefore, the prospect mold is adopted in the scheme. As the results, the proposed scheme also provides the alternate verification for the group by providing a key while at the time of encryption.

Finally in this proposed model we are just providing a solution for the existing one about the dynamic group if a user leave that group or if the user is added in to the group it is not possible to regenerate the secret information by the proposed approach we overcome this problem by simply generating the transparencies to the new users and removed user's transparencies based up on the Basis Matrix.

5. References:

[1]M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptography (EUROCRYPT'94), 1995, vol. 950, LNCS, pp. 1–12.

[2]R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam. Electron., Commun., Comput. Sci., vol. 82, pp. 2172–2177, Oct. 1999.

[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, pp. 481–494, Mar. 2004.

[4] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," J. Vis. Commun. Image Represent., vol. 21, pp. 900–916, Nov. 2010.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38,Mar. 2010.

[7]Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8]Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] F. Liu, C. K.Wu, and X. J. Lin, "Colour visual cryptography schemes," IET Inf. Security, vol. 2, no. 4, pp. 151–165, Dec. 2008.

[10] G. Horng, T. Chen, and D. S. Tsai, "Cheating in visual cryptography,"Designs, Codes, Cryptography, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[11] Sian-Jheng Lin and Wei-Ho Chung, Member, IEEE, "A Probabilistic Model of (t,n) Visual Cryptography Scheme With Dynamic Group", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[12] H. Koga, "A general formula of the -threshold visual secret sharing scheme," in Proc. 8th Int. Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, Dec. 2002, pp. 328–345.

[13] R. Z. Wang, "Region incrementing visual cryptography," IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009. [14] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes for general ," Designs, Codes, Cryptography, vol. 55, no. 1, pp. 19–35, Apr. 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

[15] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. DiscreteMath., vol. 16, no. 2, pp. 224–261, Feb. 2003.

[16] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes," Designs, Codes, Cryptography, vol. 40, no. 3, pp. 255–267,Sep. 2006.

[17] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptology, vol. 12, no. 4, pp. 261–289, 1999.

[18] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," Designs, Codes, Cryptography, vol. 35, no. 3, pp. 311–335, Jun. 2005.

[19] T.Hofmeister,M. Krause, andH. U. Simon, "Contrast-optimal out of secret sharing schemes in visual cryptography," Theoretical Comput. Sci., vol. 240, no. 2, pp. 471–485, Jun. 2000.

[20] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," Combinatorics, Probability, Comput., vol. 12, no. 3, pp. 285–299, May 2003.

[21] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of out of visual secret sharing schemes," Designs, Codes, Cryptography, vol. 11, no. 2, pp. 179–196, May 1997.

[22] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," Designs, Codes, Cryptography, vol. 25, no. 1, pp. 15–61, 2002.

[23] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," Inf. Process. Lett., vol. 110, no. 7, pp. 241–246, Mar. 2010.

[24] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," Theoretical Comput. Sci., vol. 369, no. 1, pp. 169–182, Dec. 2006.

[25] H. Hajiabolhassan and A. Cheraghi, "Bounds for visual cryptography schemes," Discrete Appl. Math., vol. 158, no. 6, pp. 659–665, Mar.2010.

[26] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, Jun. 1987.

[27] S. J. Shyu, "Image encryption by random grids," Pattern Recognit., vol. 40, no. 3, pp. 1014–1031, Mar. 2007.

[28] S. J. Shyu, "Image encryption by multiple random grids," Pattern Recognit., vol. 42, no. 7, pp. 1582–1596, Jul. 2009.

[29] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," Pattern Recognit., vol. 42, no. 9, pp. 2203–2217, Sep. 2009.

[30] N. Macon and A. Spitzbart, "Inverses of Vandermonde matrices," Amer. Math. Monthly, vol. 65, no. 2, pp. 95–100, Feb. 1958.

[31] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, Mar.
2004.

[32] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," Computer J., vol. 49, no. 1, pp. 97–107, Jan. 2006.

[33] G. B. Horng, T. G. Chen, and D. S. Tsai, "Cheating in visual cryptography," Designs, Codes, Cryptography, vol. 38, no. 2, pp. 219–236,
Feb. 2006.

[34] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," J. Vis. Commun. Image Represent., vol. 21, pp. 900–916, Nov. 2010.

[35] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[36] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

[37] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[38] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[39] F. Liu, C. K.Wu, and X. J. Lin, "Colour visual cryptography schemes," IET Inf. Security, vol. 2, no. 4, pp. 151–165, Dec. 2008.

[40] G. Horng, T. Chen, and D. S. Tsai, "Cheating in visual cryptography," Designs, Codes, Cryptography, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[41] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," IEEE Trans. Image Process., vol. 16, no. 1, pp. 36–45, Jan.2007.

6. Bibilography

- FOR .NET INSTALLATION:-
  www.support.mircosoft.com
- FOR DEPLOYMENT AND PACKING ON SERVER
  www.developer.com
  www.16seconds.com
- FOR SQL
  www.msdn.microsoft.com