www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 5, May 2014, Page No. 5796-5800

A Survey of SignCryption Its Types and Techniques

R. Bahirathy[1], S. Aruljothi[2]

[1]Lecturer, MKU Department of Computer Applications, Madurai kamaraj University
Madurai, Tamilnadu, India
bahirathyphd@gmail.com

[2]Research Scholar, Kalasalingam university Department of Computer Applications, Kalasalingam University
Madurai, Tamilnadu, India
s.aruljothi.p@gmail.com

Abstract: ***In today's internet world where nothing is protect, since the communication by transmitting of sending and receiving digital products over the open network occur very frequently the security of information is very important. Everyday so many techniques are obtaining to make message and image secure with high rate of security. Some of the encryption techniques used selective part of an image for encryption and some others apply encryption algorithm on whole image bit by bit. In this paper the existing works on the visual cryptography encryption techniques has been surveyed. Six visual cryptography encryption techniques are studied and analyzed well to analyze the performance of the encryption and decryption methods and also to ensure high rate of secure communication.***

Keywords*:* vc-visual cryptography, vcb-visual cryptography Blocks, halftoning, SK-secret key, HVS, CDS**.**

1. Introduction

In present times, the internet technology is growing high that leads a practice of process, store or share data very frequently. The protection of sensitive data like credit cards, banking transactions and social security numbers is essential. Visual Encryption techniques are used to protect these important data from unauthorized access. Data encryption is the scrambling of the content of the data, such as text, image, audio and video to make the data unreadable during transmission. Decryption is the opposite process of getting back the original data from encrypted data. Many cryptography techniques are employed, such as secret and asymmetric techniques. In this review paper different secret visual cryptography techniques are analysed. It has been analysed that the chaos based cryptography is different from cryptography algorithm. Phishing, prevention and detection systems are characterized by random behaviour, broad-band power spectrum and sensitive dependence on initial conditions. Several papers are published in the field of visual based cryptography the paper surveyed here is rather marginal. Phishing prevention and detection algorithms make it possible to explore a far greater range of potential solutions to a problem than do conventional programs.

2. Literature Survey

In this paper the architectural characteristics of many wide spread Visual cryptographic algorithms are compared and examined.

2.1 An implementation of a novel secret image sharing algorithm

In this paper, the author has proposed basic visual cryptography [1] is depends on breaking of pixel into some sub – pixels or we can say extension of pixels. Every pixel from the secret image is encoded in to multiple sub pixels in every share image using a matrix to fix the color of the pixels. In this paper the author has taken the three type of method first method is the binary secret image sharing method. In this method an image that has only two feasible values for every pixel basically the two colors obtained for a binary image are black and white every pixel is considered as a single bit 1 or 0 for binary image, arrange to obtain the proposed scheme [2]. The gray scale level (k) should be getting as 2. The rest of the procedure is similar for construction of shares and revealing phase of retrieve the secret image in this method the author has processed to many process [3].

2.1.1 Sharing process

To carry take the pixels of a binary image of h x w dimension. For each pixel denote whether it is black or white. Now for each pixel, we get a random function to take a set of pixels from the code book which present two set of pixels for every selection pixel one considering to share – 1 while other considering to share – 2 of the image. At the last step two share of size h * 2 w are created

2.1.2 Re-construction process

Take both the shared images to rebuild the original binary image. Collecting the related pixels from both the shared images we create a new pixel by executing the following operation ~ (A + B). A is the pixel from share –1, "+" denote the binary or operation, and "~" denote the binary negotiation (Not) operation. The author has taken the second method is gray scale secret image.

2.1.3 Share construction

Get mixed image PA by using a key to create a permutation sequence to permute the pixels of A generates n-1 random matrices. R_1-----R_{n-1}, each of his size h x w and element be (0, K–1) for an image with K gray scale levels. Next calculate $R_n = (K_j - R_1\text{-----}R_{n-1}) \bmod K$, $S_i = (R_i + PA) \bmod K$, $S_n = (R_n + K_j - (n-2)PA) \bmod K$ here, j is the unit matrix the size of h x w "+" and "-" means corresponding matrix addition and matrix addition and matrix subtraction.

2.1.4 Image reconstruction

In this process the author has first to calculate the $PA = (S_1 + \ldots + S_n)$ next apply inverse scrambling operation to PA_1 to get the reconstructed image A_1.

2.1.5 Color secret image sharing method

In this method has taken any requested colors can be get by combining primitive colors red (R), green (G) and blue (B). Which is denoted by 8 bits and 0.255 variation of scale. To expand the proposed method for gray scale image to color image, three steps are required. Firstly, decompose the color image in to three elements of R, G and B, each of which can be looked as gray scale image then execute the proposed scheme for gray scale image to every element R, G and B. At last compose R, G and B elements to create shares. In the revealing phase, again take the decomposed RGB elements of the shares and perform the proposed scheme individually at join to create the RGB elements to reconstruct the secret image. To examine the proposed method of binary image, gray scale image and color image has applied the two shares, and final reconstructed original image from those two shares.

2.2 Image captcha based authentication using visual cryptography

In this paper, the author has introduced the new algorithm to find the phishing website [4]. This algorithm is depends on the anti phishing image captcha validation scheme using visual cryptography. It protects the password and other important information from the phishing websites.

The proposed approach can be divided in to two phases' registration phase and login phase

2.2.1 Registration phase

In this phase, a key string (Password) is requested from the user at the time of registration for the secure website. The key string can be a mixing of alphabets and numbers to give safer environment[5]. The key provided by the user this string is joined with randomly created. String in the server and an image captcha is created. So the new image captcha is worked rear. So the new image captcha is worked rear. By the dynamic creation the steal by camera can be easily avoided. Then the "blowfish algorithm" is used to divide the original image captcha in too many blocks and re modified, Then"Splitting and rotating algorithm" is used to rotate the re modified blocks. The image captcha is divided in to two shares by (2,2) visual cryptography method such that the image captcha is divided according to black and white pixels. Then one of the shares is put with the user and the other share is put in the server. The user's share and the original image captcha is sent to the user for verification throughout the login phase. The image captcha is also stored in the actual database of any important website as important data due to the image captcha is applied as the password later. After the registration, the user can modify the key string continuous change when it is required[6].

2.2.2 Login phase

When the user logs in by get in his important information for applying his account, then first the user is requested to enter his user name (user id). Then the user is requested to enter his share which is stored. This share is sent to the server where the user's share and share which is kept in the data base of the website for each user, is stacked joint to produce the image captcha. The image captcha is shown to the user. The end user can verify whether the shown image captcha image captcha matches with the captcha generated at the time of registration. The end user is needed to enter the text shown in the image captcha and this can service the purpose of password and using this, the user can give in to the website. Using the username and image captcha created by stacking two shares one can check whether the website is protect website or a phishing website and can also check whether the user is a human user or not. When user try to login in to site in order to increase more security the image captcha is encrypted. The encryption phase include many algorithms like blow fish, splitting and rotating algorithm

and (2,2) vishual cryptography scheme blow fish "algorithm" is used to the original image captcha then the image captcha is divided into many blocks and modified after the image captcha blocks are modified, the "splitting and rotating algorithm" is used to the image captcha, then the modified and rotated blocks. Are joined then (2,2) VCS scheme is used to the mixed blocks. This scheme is applied to divide the encrypted image captcha in to two shares based on white and black pixels. When the two sub pixels are same blocks it regard as a white pixel. When the two sub pixels are distinct the original pixel is regard as black pixel. This VCS scheme adds more complexity to the image captcha finally one of the share is stored with user and another part of the share is stored with server. When two shares are stacked combine and the reverse process of encryption taken place the original image captcha is shown from this user can verify whether the website is original or fake. At the similar time the server can check whether the user is human being or robot. To examine this methodology is used to encryption process to compute the block transformation, rotation and subpixel divIdence and use to login to the website.

2.3 Visual cryptography for gray scale Image Using Block Replacement Half Toning Method

In this paper the author has taken the appropriate large size of the image[7]. When use the block replacement method for halftoning, the size of halftoned image get the double the size of source image. Next we use normal (n,n) visual cryptographic image of pixel extension m=4(sub pixel) then the size of shares maked after encryption get too large[5]. Handling these large size shares is slow process. Source image received by superposing these n shares is not visible by human visual system we use particular (n,n) visual cryptographic scheme proposed. Which is applied to handle large size source image. Decryption demands n shares for obtaining source image. It is preferable for high security. The author used the Block Replacement Algorithm for Halftoning a gray level image to Bi-level image. Each pixel in the original image is changed by a 2X2 matrix [8].

Next the author used the Visual Cryptography based on Alignment of Shares for producing encrypted shares for halftone image. Using this mechanism to examine the result using sharing concept and again reconstruct the original image [9]. It is proved that give the more secure for both encryption and decryption method.

2.4 A Cryptographic Image Encryption Technique For Facial-Blurring of Images

In this paper, the author has chosen the facial portion of the image utilized will have their RGB colors pullout from then and then encrypted to get a ciphered image partition[10]. The ciphering of the image for this paper will be made by applying the RGB pixel values at the chosen portion of the images. There are no modification of the bit values and there is no pixel development at the end of the encryption process. Replace the numerical values are transposed, reshaped and concatenated with RGB values shifted away from its corresponding positions and the RGB values exchanged in order to get the cipher image. This implies that, the total change in the sum of all values in the image is zero. The image is appeared at as a decomposed translation in which the three principle element [11]. Which forms the image is selected to perform upon by the algorithm. The RGB elements can be regarded as the trio that forms the qualifications of a pixel. The pixel is the smallest component of an image which can be separated and still include the qualification establish in the image. The RGB values are shifted out of its original pixel and exchanged within the image boundaries by the algorithmic process. The shift removal of the R, G and B values known called as the element removal factor array which is distinct for R, G and B. With the proposed method in this paper, the shuffling of the image will be made done by only moving the RGB pixels and also exchanging the RGB pixel values.

In the Encryption method, first take the data from the obtained portion and generate an image graphics object by interpreting each element in a matrix [12]. Then extract the red component as 'r', green component as 'g' and blue component as 'b'. Finally get the size of r as [c, p]. Now let r is a transpose of r, g is transpose of g and b transpose of b. Then reshape r into (r, c, p), g reshape into (g, c and p), next b reshape into (b, c and p). Next perform the Concatenate the arrays r, g, b into the same dimension of 'r' or 'g' or 'b' of the original image. At last data will be changed into an image format to obtain the encrypted image. The inverse of the algorithm will decrypt the encrypted image back into the plain image. In this paper the author solved the algorithm using mathematical explanation. To analyze this mechanism provide more secure for the image visual cryptography against all possible attacks.

2.5 A Visual Cryptographic Encryption Techniques for Securing Medical Images

In this paper, the author has used the encryption process, an input image which was a plain image was worked on by a method to create a secret key from it [13]. The key was then applied to encrypt the image by shuffling the pixels of the plain image depends on an algorithm. The ciphered image was get at the end and it can either be stored or transmitted through a communication network. The received image was then worked on anew by a method to get the key in order to decrypt the image. First the author taken the plain image P1 and the ciphered image is C1. Sk is the secret key applied in the encryption and the decryption process of the image. In the encryption process, the images employed had their RGB

colors shuffled to get ciphered images. The ciphering of the images for this research was based only on the RGB pixel values of the images and the secret key get from the image. There were no alter of the bit values of the images employed and there was no pixel extension at the end of the encryption and the decryption process. The numerical values of the pixels were removed from their corresponding location and the RGB values were exchanged in order to get the ciphered images. This express that, the total modification in the sum of all values in the image was zero. There was no modification in the total size of the image during encryption and decryption process. The distinctive quality sizes of image kept un exchanged during the encryption process[14].

The following proposed algorithm steps is used to describe both encryption and decryption method. To take the data from image and create an image graphics object by explaining each element in a matrix. To obtain the size of r as [c, p]. Next obtain the Entropy of the plain image. Calculate the Mean value for plain Image. And calculate the shared secret from the image. To repeat the step using the secret key value. And perform the Extract operation for the Red, Green and Blue (r, g and b). Let r Transpose of r and g Transpose of g then b Transpose of b. Next reshape rgb image into corresponding (r, c, p), (g, c and p) and (b, c and p). Then perform the Concatenate operation of the corresponding array values like r, g, b. At last the date will be changed into an image format to obtain the encrypted image.

We can get the Sk secret key is getting using Sk=[(cXp) + |(He X 10^3)| + |(x'=1/n.$\sum$xi)|]mod p. Here the c, p are dimension of the image and He is the entropy value of the image and x dash is the arithmetic mean for all the pixels in the image. To examine this techniques proven that the more secure for the both encryption and decryption method [15].

2.6 Visual Cryptography for Gray-scale Images Using Bit-Level

In this paper, the author to encrypt a gray scale image two gray-scale shares, the original image is resolved into eight bit planes[16]. Every bit plane is encrypted using binary visual cryptography. All the encrypted shares of the bit planes are reconstructed and two gray scale shares are generated. Superimposing gray-scale shares expose the secret. The algorithm to describe our proposed method exactly. The original image with size m x n is entirely scanned. Two gray scale shares S1 and S2 are denoted with size 2m x 2n[14]. Then every bit b in values of (2i-1,2j-1)-(2i,2j) pixels is S1 and S2 is assigned, related to bit b in value of pixel (i,j) in the original image. 2 x 2 Matrices A_1-A_8 are bit planes A. A_1 denote the least and A_8 is the most significant bit plane[17]. Each of A's bit planes can be encrypted using binary VC that results a set of eight binary to A's bit Planes. It is arbitrarily chosen the matrix and its complementary is also placed. Because the value of $A_1(1,1)$ is Zero. Repeat the process until the $E_{2,8}$ matrices.In printing process, first printed black pixels obtain get a value of one, because there is in k to analyze the light and printed white pixels get a value for zero. HVS performs binary OR operation on two shares because on superposition, if the pixel is black at least in one share, the light is analyzed and HVS views the result as black, and only if both of the pixels are white, it is seem as white. This represent is executed reversely in CDS. As for black pixels, light is not projected (0 value) and for white pixels, light is projected (1 value). HVS should be substituted by AND operation in the CDS. Superimposing $E_{1,k}$ and $E_{2,k}$ results R_k (k is the index of bit plane) as the AND operation is used to them. Every 2 x 2 sub – matrix in R_k represents the original value in A_k. Reconstructing these matrices, as they are decomposed, results matrix R as a representation of matrix A in retrieval phase. To examine the techniques applied encrypted binary share images created by VC. The result superimposing those encrypted planes. In this method also provide more secure both encryption and decryption techniques [18].

3 Conclusions

From the analysis it has been observed that which one is the best approach to calculate these things. Also focuses on visual image encryption techniques, information encryption techniques and phishing prevention and detection encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues. We conclude that all techniques are suitable for different applications and unique in its way with advantages and limitations. The future enhancement of the work is going to examine the encrypted image using some attack like rotation attack, noise pepper attack etc and can be assigned for multimedia data.

References

[1] Shanu Sharma,**"**An implementation of a novel secret image sharing algorithm", IJCSMC, Vol. 2, Issue. 4, April 2013, pg.263 – 268.

[2] Bhaskar Mondal, Deep Sinha and Navin Kumar Gupta, Nishant Kumar and Pankaj Goyal, "An Optimal (n,n) Secret Image sharing Scheme", UACEE International Journal of Computer Science and its Applications Volume 2: Issue 3, 2012, pp 61-66.

[3] Lin Dong, Min Ku, "Novel (n,n) secret image sharing scheme based on addition", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010, iih-msp, pp.583-586.

[4] A.Angel Freeda, M.Sindhuja and K.Sujitha, "Image captcha based authentication using visual cryptography", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013.

[5] M. Naor and A. Shamir, "Visual cryptography", Proc. Eurocrypt, 1994, pp. 1–12.

[6] A. Shamir, "How to Share a Secret Communication", ACM, vol. 22, 1979, pp. 612-613.

[7] Abhishek Kr Mishra and Ashutosh Gupta "Visual cryptography for gray scale Image Using Block Replacement Half Toning Method", African Journal of Computing & ICT, Vol 6. No. 4, October 2013.
[8] Abhishek Kr Mishra, Ashutosh Gupta, AshishKumar, "(n, n) Visual Cryptography based on Alignment of Shares, International Journal of Computer Applications (0975 – 8887)" Volume 60–No.18, December 2012.
[9] Sadan Ekdemir, Xunxun Wu, "Digital Halftoning Improvements on the Two-by-Two Block Replacement Method", UPPSALA university, Project in Computational Science", Report January 2011.
[10] Quist-Aphetsi Kester, MIEEE, Lecturer Faculty of Informatics, Ghana Technology University College, PMB 100 Accra North, Ghana, "A Cryptographic Image Encryption Technique for Facial-Blurring OF Images" International Journal of Advanced Technology & Engineering Research (IJATER), ISSN No: 2250-3536 Volume 3, Issue 3, May 2013.
[11] Shujiang Xu,Yinglong Wang,Yucui Guo,Cong Wang, "A Novel Image Encryption Scheme based on a nonlinear Chaotic Map", IJIGSP, vol.2, no.1, pp.61-68, 2010.
[12] Ruisong Ye,Wei Zhou,"A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", IJCNIS, vol.4, no.1, pp.38-44, 2012.
[13] Quist-Aphetsi Kester, MIEEE Faculty of Informatics, Ghana Technology University College, PMB 100 Accra-Norths, Tesano, Accra, Ghana, "A Visual Cryptographic Encryption Techniques for Securing Medical Images", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 6, June (2013).
[14] Quist-Aphetsi Kester,"Image Encryption based on the RGB pixel Transposition and Shuffling", IJCNIS, vol.5, no.7, pp.43-50,2013.
[15] Quist-Aphetsi Kester,"Image Encryption based on the RGB pixel Transposition and Shuffling", IJCNIS, vol.5, no.7, pp.43-50,2013. DOI: 10.5815/ijcnis.2013.07.05.
[16] D. Taghaddos and A. Latif, "Visual Cryptography for Gray-scale Images Using Bit-Level", Journal of Information Hiding and Multimedia Signal Processing Ubiquitous International, Volume 5, Number 1, January 2014.
[17] A. Latif, and A. R. Naghsh-Nilchi, "Digital image watermarking based on parameters amelioration of parametric slant-hadamart transform using genetic algorithm", International Journal of Innovative Computing, Information and Control, vol. 8, no. 2, pp. 1205-1220, 2012.
[18] F. Liu, T. Guo, C. K. Wu, and L. Qian, Improving the visual quality of size invariant visual cryptography scheme, Journal of Visual Communication and Image Representation, vol. 23, no. 2, pp. 331-342, 2012.