ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

A Novel Approach on Color Extended Visual Cryptography for General Access Structures using Error Diffusion

Shekha Chenthara[1], Deepika M.P[2], Dr. Varghese Paul[3]

M.Tech., Student, CSE, AdiShankara Institute of Engineering and Technology, Kalady, India[1]

Head of the Department, IT, AdiShankara Institute of Engineering and Technology, Kalady, India[2]

Dean, CS IT, Cochin University of Science and Technology, Cochin, India[3]

Abstract: This thesis proposes a novel approach on color extended visual cryptography for General access structures using the principle of Error diffusion. Conventional visual secret sharing schemes suffers from a management problem, so that dealers cannot identify each share visually. This problem can be solved by the extended visual cryptography scheme (EVCS) by adding a meaningful cover image in each share. The previous approaches involving the EVCS for GAS suffers from a pixel expansion problem and also needs a sophisticated codebook design for various encryption schemes. This paper proposes a general approach to solve the above mentioned problems. This approach can be used for color secret images in non computer aided decryption environments. Color Extended VC encrypts a color secret message or image into color halftone shares. This paper proposes a novel encryption algorithm for the encryption of color secret message using the concept of Jarvis Error diffusion halftoning using Jarvis matrix permutation and Inverse Halftoning using Neural network based method. In visual secret sharing based on Halftone VC, the continuous halftone image is first transformed in to a halftone image and then encrypted using extended VSS. These halftone shares are then error diffused concurrently to give visually pleasing effect. The proposed approach consists of two phases. The first phase of the algorithm based on a given access structure, constructs a set of pixel-expansion-free shares using Jarvis Error diffusion Halftoning. The second phase of the algorithm adds a cover image on each share directly via stamping algorithm based on LSB replacement thereby removing the pixel expansion entirely. In the stamping algorithm, Secret image can be hiding itself in the cover image. Finally secret image will be perfectly reconstructed by inverse halftoning algorithm using neural network method. Secret image can be reconstructed by stacking the qualified set. Comparisons with previous approaches show the superior performance of this newly proposed method.

Keywords: EVCS;GAS;LSB;HT;VSS

I. INTRODUCTION

Visual cryptography was proposed by Naor and Shamir [1], allows the encryption of secret information in the image form. In the concept of secret sharing, a secret image can be encrypted as n different share images printed on transparencies, which are then distributed to n participants. By stacking transparencies (shares) directly, the secret images can be revealed and visually recognized by humans without any computational devices and cryptographic knowledge. On the other hand, any one share or a portion of shares can leak nothing related to the secret image .VC is a very good solution for sharing secrets when computers cannot be employed for the decryption process. Later on threshold visual secret sharing scheme, also known as k-out-of-n VSS scheme or(k,n)-VSS scheme[2] have been proposed. Ateniese [9] proposed the concept of general access structure (GAS) and also developed a VC-based solution for some GASs.By using the GAS [9], dealers can define reasonable combinations of shares as decryption Conditions rather than specifying the number of shares. Hence, the (k, n)-VSS scheme can be treated as a special case of the GAS. Conventional VSS [2] schemes generate noise-like random pixels on shares to hide secret images. So, the secret can be perfectly concealed on the share images. These schemes suffer from a management problem so that dealers cannot identify each share visually. The pixel expansion problem [10] is also a common disadvantage with most of the VSS schemes. When the VC-based approach is employed, each secret pixel within a secret image is encrypted in a block consisting of 'm' sub pixels in each constituent share image. Thus, the area of a share is 'm' times that of the original secret image. Thereby contrast of the recovered images will be decreased to '1/m' simultaneously. The pixel expansion problem not only affects the practicability of storage and transmission requirements for shares but also decreases the contrast of the recovered secret images. So developed a friendly VC scheme known as the extended visual cryptography scheme, which adds a meaningful cover image on each share to address the management problem and the pixel expansion problem.

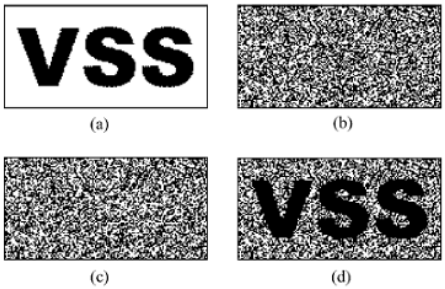

Fig 1: Example for Visual Cryptographic Scheme
(a) Secret Image (b) Share1 (c) Share2 (d) Stacked Result

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

II. BACKGROUND AND RELATED WORK

A. An Extended VC Algorithm for General Access Structure

This paper proposes a new method that resolves management problem; pixel expansion problem. This approach can be used for binary secret images in noncomputer aided decryption environments. The proposed approach consists of two phases. The first phase of the algorithm uses optimization technique for a given access structure, constructs a set of noise like shares that are pixel-expansion-free. This phase identifies and formulates the problem as a combinatorial optimization problem and then developed a simulated-annealing [7] based algorithm to solve it. The second phase of the algorithm directly adds a cover image on each share directly via a stamping algorithm and thereby removing the pixel expansion entirely. The experimental results shows that this approach is a solution to the pixel expansion problem of the EVCS. Moreover, the display quality of the recovered image is very close to that obtained using conventional VC schemes.

B. A Fast Encryption Algorithm for Color Extended Visual Cryptography

In this paper, an Error Diffusion Halftoning algorithm [16] to generate color shares for color secret image has been proposed along with other techniques. Here the secret color image is decomposed into its single color components R,G,B. This phase generates shares by using the error diffusion algorithm. Error diffusion will generates halftone shares with high quality. It measures every pixel using a neighborhood operation. Error diffusion scans the secret image one row and one pixel at a time. At every step, the algorithm compares the grayscale value of the current pixel J(i, j) which is represented by an integer between 0 and 255, to some threshold value ie 128 r 127. If the grayscale value is greater than the threshold value, the output pixel I (i, j) is considered black (value 0) otherwise it is considered white (value 1). The difference between the pixel's original grayscale value and the threshold is considered as an error. Error is calculated which will be the difference between original image and halftone image. The error calculated will be then added to the next pixel in the image and then the process continues. The error is then added to which neighbor is decided by an error diffusion matrix named Jarvis mask or Jarvis matrix.

C. Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based (k,n)-VCS

A new secret sharing scheme with meaningful shares using (k,n)-threshold visual cryptography and digital watermarking for grayscale images based on bit plane encoding is proposed in this method. Initially, an image is decomposed into its bit plane images that generate a binary image at each bit plane. Secondly, the traditional binary secret sharing scheme is used to get the sharing images. Finally, a proposed watermarking technique is used to generate meaningful shares. To decrypt hidden secret image, extract the shares from the cover image and decompose each share into bit planes and then secret grayscale image is reconstructed. This scheme provides a more efficient way to hide images in different meaningful shares. To reduce the interest of hackers, we have proposed a technique called digital enveloping. This is nothing but an extended invisible digital watermarking technique. Using this technique, the shares, produced by k-n secret sharing visual cryptography are embedded into the envelope images by LSB replacement [19]. This can be done by replacing the b Least Significant Bits (LSB) of each channel represented with 8 bits of the 24-bit color image.

D. Inverse Halftoning Using Neural Networks based methods

The halftoning is one of the binarization techniques that convert gray-scale image into a binary image. The technique of reconstruction of a corresponding gray-scale image from a given binary halftone image is called inverse halftoning. This paper proposes a neural networks based inverse halftoning methods, which are Multilayer Perceptron (MLP)-based inverse half toning method[20]. In this method, the training stage is required using some halftone images and their corresponding gray-scale images. However once both neural networks are trained, the adapted connection weight values can be used to generate gray-scale images from any unknown halftone images in training stage. The proposed methods provide the higher quality gray-scale images compared with the previous methods.

III. PROPOSED WORK

Solution Procedure for Proposed Method

This method uses a two-phased encryption algorithm of (Tqual,Tforb) -EVCS for GASs.In the first phase, an Error Diffusion Halftoning algorithm is used to generate color shares for color secret image.Here image is decomposed into its single color components R,G,B.Those components individually are continuous gray scale in which we can perform cryptographic computations.Error diffusion will generates halftone shares with high quality.Then it generates intermediate basis shares (S1,. . . .,Sn)of (Tqual,Tforb)-VCS using Yang's ProbVSS and synthesize those shares using synthesizer.These intermediate shares (I-shares) have a meaningless appearance and no pixel expansion.In the second phase,cover images itself will stamp together using LSB replacement watermarking algorithm produces the resultant secret image.

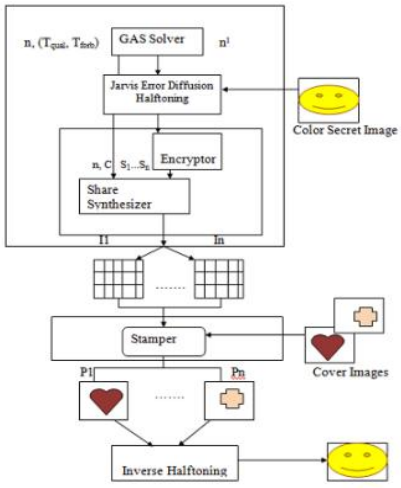

Fig 1: Solution Procedure

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

A. Phase 1-Generating I-Shares

This phase 1 of this method aims to construct a pixel expansion-free VCS for a given access structure (Tqual, Tforb). The idea behind the solution is as follows. A security system employs n' different keys to protect a secret and distributes these keys to n different participants. Each and every key may be duplicated and will be distributed to at least one participant. Each participant is allowed to hold at least one key.

If someone wants to access the secret, he/she has to collect n' different keys from a set of participants. If he/she misses any one type of key, the secret will remain protected. So for an access structure(Tqual, Tforb)the dealer has to carefully distribute n' different keys to any set of participants X,X ЄTqual and has to guarantee that any set of participants Y, YЄTforb, will not hold all types of keys.

In summary, phase I of the proposed algorithm contains two sub procedures: First, finding the number of basis n' shares and a corresponding construction set C for a (Tqual,Tforb)- VCS.We develop a GAS solver to deal with these works. Before Encryption we need to halftone the color secret image in to binary image and generate color meaningful shares R,G,B with the proposed scheme. During this phase an Error Diffusion Halftoning algorithm is used to halftone the Secret Image. Second, basis shares S1,...,Sn that were yielded by constructions of (n',n')-VCS and the construction set C will be utilized to obtain uncovered I-shares.

This work will be carried out by the encryptor using Yang's probabilistic vss scheme and the share synthesizer. In the 2nd phase, a stamping algorithm based on LSB replacement in which cover images itself will stamp together produces the resultant secret image.

During that phase an Inverse Halftoning algorithm using Neural Network method is used for generating the secret image. The proposed methods offer a high quality of secret image compared with the previous schemes.

B. GAS Solver-General Access Structure Solver

For a set of participants P= {i1,i2,….in} and access structure (ΓQual , ΓForb) the GAS solver is used to finding a construction set C with minimal n^1.In this section, we develop an algorithm based on the simulated annealing approach to solve the proposed mathematic optimization formulation for the GAS problem. Inorder to simplify optimization procedures, use penalized energy function in the model. The penalized energy function Ep can be defined as Ep= Nf + |TQual| / (1 + Nq) where Nq denotes the amount of a set that can recover the secret image and Nf represents the amount of an insecure forbidden set in TForb.

Our solution approach adopts an iterative improvement framework. The iteration is based on the decision variable n^1. The proposed iterative improvement framework is listed in Algorithm 1. The pseudo code for the proposed SA-based algorithm, GAS_SA() is in Ref [10].

Algorithm 1: SA based algorithm for GAS Solver

```
Procedure GAS_solver (n,n1max, TQual,TForb)
1. n1← n
2. Call GAS_SA(n,n1,TQual,TForb,Cbest,Zbest)
3. If Zbest ≥1 then   // No solution in last turn
4. n1←  n1+1
5. IF n1= n1max then Stop and Output  "No solution found"
6. If n1 < n then goto Step 11
 Else
7. C ←Cbest . //  Found a solution in last turn
8. If n1 > n then goto Step 11
9. n1←n1-1 // Improvement
10. End If
11. Goto Step 2
12. Output n1, C
```

C. Halftoning Using Error Diffusion

During this phase, Error Diffusion Halftoning algorithm is used to generate color shares for color secret image. Halftoning is a binarization technique that converts gray scale image into a binary image in which it converts gray scale pixel into binary one using a threshold value. The proposed system uses color image as secret image. So some halftoning techniques are applied before encryption. In this stage the color secret image is separated into three planes R, G, B. Then halftone operation is performed in each plane separately. Half toned R, G, B planes are given to the encryptor. In halftoning the greyscale image is converted into binary images.

So after halftone operation three binary images are obtained. Error diffusion will generates halftone shares with high quality. It measures every pixel using a neighborhood operation. Error diffusion scans the secret image one row and one pixel at a time. At every step, the algorithm compares the grayscale value of the current pixel J(i, j) which is represented by an integer between 0 and 255, to some threshold value ie 128 or 127. If the grayscale value is greater than the threshold value, the output pixel I(i, j) is considered black (value 0)otherwise it is considered white (value 1).

The difference between the pixel's original grayscale value and the threshold is considered as an error. Error is calculated which will be the difference between original image and halftone image. The error calculated will be then added to the next pixel in the image and then the process continues. The error is then added to which neighbor is decided by an error diffusion matrix named Jarvis mask or Jarvis error diffusion matrix.

```
Procedure JARVIS ERROR DIFFUSION
1. Procedure Halftoning_image
2. for i = 1,. . . . . ,n do
3. for j = 1,. . . .,m do
4. if J(i, j) < 128 is found then J(i, j) = 0
5. else J(i, j) = 1
6. error = J[i, j] - I[i, j]*255
7. Distribute error to the right pixel
8. Distribute error to right diagonal pixel
9. Distribute error to the bottom pixel
10. Distribute error to the left diagonal pixel
11. After the error has been diffused the pixel value of
the next position is compared to threshold and process
repeats till all pixels are finished.
12. end for
13. end for
14. end procedure
```

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

D. Algorithm for Share Constructor

The share constructor consists of two modules in Figure 1: the encryptor and share synthesizer. The encryptor adopts Yang's construction for the (n^1,n^1) – ProbVSS scheme. In the share constructor, encryptor generates the basis shares by employing Yang's ProbVSS scheme. Then the share synthesizer produces intermediate shares (I- shares) by stacking the basis shares upon the construction set C. The procedure for the share constructor is described in Ref [10]. The share constructor phase is applied on three planes.

E. Phase II-Stamping

After generating color shares using Error diffusion halftoning algorithm, those color shares are encrypted using Yang's Prob VSS scheme and synthesized, ie distributes those shares to corresponding P participants. In the 2nd phase,a stamping algorithm is used in which cover images itself will stamp together produces the resultant secret image. If the random looking shares are enveloped into meaningful images using cover images, the interest of hackers can be reduced, thereby providing more security to visual cryptography. Otherwise hackers thought that it might be a critical information. Therefore here used a technique called digital enveloping or stamping or embedding of cover images into shares using LSB replacement.

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message.LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value.It is clear that on average, only half the LSBs need to change.The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.Results show a cover image and a stego image with data is embedded, there is no visible difference between the two images.LSB matching randomly increments or decrements the data value by one. LSB matching is also known as ±1 embedding .

Algorithm 3: Proposed Stamping Algorithm

1. Repeat for all shares
2. Repeat for each pixel of share
(i) Generate an array S[0.....8] that contain the bits of the pixel value.
(ii) Decompose the cover image into three component such as Red, Green, and Blue and then store the bits of each component into three arrays R[0...8], G[0...8], and B[0...8] respectively.
(iii) Find that which channel can contain more information i.e. which color has less effect in the cover image.
(iv) Replace the least significant bits of rest two channels with the share pixel value that have less effect.
3. Stop.

F.Proposed Inverse Halftoning Decryption Algorithm

The extracting of secret image is done using Inverse Halftoning algorithm using Neural network based method. The technique of reconstruction of a corresponding gray-scale image or a color image from a given binary halftone image is called inverse halftoning. Stack operation can be implemented by performing the OR operation to reveal the secret image.

It makes use of MLP-based inverse halftoning method to associate between binary input data and output gray scale data. Each pixel is considered as a center pixel whose gray scale value will be estimated during training stage providing gray scale value of center pixel as the desired data. It makes use of different blocks of 4x4 matrix. Once the MLP is trained, halftone images are introduced to the trained MLP to get gray-scale images with better quality. Then the final secret image will be retrieved by reconstructing using qualified participants.

IV. OBSERVATIONS AND RESULTS

The simulation was done in MATLAB, evaluating the performance and the quality. In color extended Visual Cryptography, Analysis is performed by calculating Contrast. Since there is no pixel expansion, pixel expansion factor is 1. Contrast is the difference in luminance or color that makes an object or its representation in an image or display distinguishable. The maximum contrast of an image is the contrast ratio or dynamic range.In Binary images we can calculate contrast using counting the value of number of Ones. equation:(No of ones/Total number of pixels)*100

Secret Image	Qualified Set	n'	Construction set C	Pixel expansion	Contrast
CSIE RMI	12,13,14,23,24	3	{{s1,s3},{s2,s3},{s1,s2},{s1,s2}	1	20.97%
VSS	12,13	2	{{s1},{s2},{s2}}	1	45.85%
Color Secret Image	12,13,14,23,24	3	{{s1,s3},{s2,s3},{s1,s2},{s1,s2}	1	67%

Table 1: Analysis of Color Extended Visual Cryptographic scheme

V. CONCLUSION

This thesis proposed a two-phased encryption algorithm for the EVCS for general access structures. It makes use of a jarvis error diffusion halftoning algorithm for generating color shares and also used LSB replacement for stamping cover images, Error diffusion is a procedure that also produces pleasing halftone images to human vision. It is an efficient method that implements color Extended visual cryptography for general access structures using error diffusion that eliminates all the problems with existing EVC schemes.

Results show that ,our approach has better performances than in previous research in terms of display quality of the recovered image, contrast, perfect reconstruction of secret pixels, and maintenance of the same aspect ratio as that of the original secret image. The proposed algorithm has some advantages. First, the algorithm is a generic approach. It can construct the color EVCS for general access structures without the need to design a sophisticated codebook. The second advantage is the modularity. Each phase in the encryption procedure is less coherent, so it can be individually designed and also can be replaced separately. The third advantage is the first phase of the proposed algorithm: this phase is applicable not only to the extended

color VC schemes but also to the conventional color VC schemes. The fourth advantage is that it removes the dimtraces of cover images on the recovered images in the previous EVCS scheme. This is a simple and efficient Visual Cryptographic scheme that adds security for secure communication.

VI. FUTURE WORK

In this proposed method, when the key value increases the contrast of recovered images is reduced. A study for increasing the contrast can be studied as a future work. During stamping, this method have used a single cover image for each shares. It can also be studied as a future work by using a pair of cover images to ensure security. Other disadvantage with the proposed thesis is that it is taking some time during the reconstruction of secret image. Fast retrieval of secret image in minimum time can also be studied as a future work.

REFERENCES

[1] M.Naor and A.Shamir, "Visual Cryptography", in Proc.EUROCRYPT, 1994, pp.1-12
[2] [E. R. Verheul and H. C. A. v. Tilborg, Constructions and properties of k-out-of-n visual secret sharing schemes, Designs Codes Crypto., vol. 11, pp. 179_196, 1997
[3] A. Adhikari and S. Sikdar, A new (2, n)-visual threshold scheme for color images in Proc. INDOCRYPT 2003, Berlin, Germany, 2003
[4] C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, Contrast optimal threshold visual cryptography schemes"SIAMJ Discrete Math., vol. 16, pp. 224_261, 2003
[5] C. N. Yang, New visual secret sharing schemes using probabilistic method,Pattern Recognit. Lett., vol. 25, pp. 481_494, 2004
[6] C. Blundo, S. Cimato, and A. D. Santis,Visual cryptography schemes with optimal pixel expansion, Theor. Comput. Sci., vol. 369, pp. 169_182, 2006
[7] P. L. Chiu and K.H.Lee,A simulated annealing algorithm for general threshold visual cryptography schemes IEEE Trans. Inf. Forenics Security, vol. 6,Sep. 2011
[8] Mizuho Nakajima,Yasushi yamaguchi,university of Tokyo,Extended visual cryptography for natural images
[9] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Visual cryptography for general access structures, Inform. Comput., vol. 129, pp.86_106, 1996
[10] Kai-Hui-Lee and Pei-Ling-chui,An extended visual cryptographic algorithm for general access structures,IEEE February 2012
[11] InKoo Kang,Gonzalo R.Arce,heung-Kyu Lee, Color Extended Visual Cryptography Using Error Diffusion, IEEE Trans. On Image processing,vol.20
[12] Feng Liu,Chuankun Wu, and Xijun Lin, _Step Construction of visual cryptography schemes, IEEE Transactions On Information Forensics And Security, Vol. 5, No. 1,March 2010
[13] Pankaja Patil , Bharati Pannyagol ,Visual Cryptography for color images using Error diffusion and Pixel synchronization,International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 1 Issue 2 July 2012
[14] Dr.D.Vasumathi ,M.Surya Prakash Rao, M.Upendra Kumar, Dr.Y.Ramadevi,Dr.R.Rajeswara Rao, Novel Approach for Color Extended Visual Cryptography Using Error Diffusion,International Journal of Computer Trends and Technology vol.3 Issue4-2012
[15] Nitty Sarah Alex,L. Jani Anbarasi, Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography,2011 IEEE
[16] Anuprita Mande, Manish Tibdewal , A Fast Encryption Algorithm for Color Extended Visual cryptography,International Journal of Emerging Technology and Advanced Engineering,Volume 3, Issue 4, April 2013
[17] Prof.S.S.Asole, Ms. S.M.Mundada,_Securing Databases from Unauthorized Users ,International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013
[18] Chandramathi S, Ramesh Kumar R., Suresh R and Harish S, An overview of visual cryptography, International Journal of Computational Intelligence Techniques
[19] Aarti,Harsh K Verma,Pushpendra K Rajput , "Ideal Contrast Secret Sharing Scheme through Meaningful Shares with Enveloping Digital Watermarking using Bit Plane based(k,n)-VCS"
[20] F.Pelcastre-jimenez,L.Rosales-roldan,M.Nakano-miyatake,H.Perez-meana ,Inverse Halftoning using Neural Networks based methods ,Advances in Circuits, Systems, Automation and Mechanics