I J C T A, 9(9), 2016, pp. 3621-3628

A New Hypervising Technique Image Stamper Synthesizing Technique for Secure Visual Sharing

Robert[1], Celine Kavidha[2] and Jebisha Arul[3]

ABSTRACT

This paper discusses a solution to improve the quality of the original visual which has been shared between the data owner and the user in an secured manner using two step share synthesize image stamper algorithm. The dealers are facing the problem in administration side, since they cannot find their shares visually. This situation happens because, to hide the secret visual, noise-like (dots) random pixels are generated using conventional visual secret sharing schemes. A meaningful cover image[1] is added to convert the meaningless share to the meaningful share by using extended visual cryptography scheme (EVCS) to overcome the problem of unidentified share which causes confusion in the system. Even after doing all these processes, EVCS approach which was previously used with the general access structures experienced the pixel expansion problem. Two phases are used in the proposed approach. The construction of the meaningless shares with the help of the optimization technique, in the initial phase the creation for conventional VC schemes can be done based on the hierarchical structure given in access structure form. In the next phase, the meaningful images are to be added as cover image respectively in each and every share in the partitioned system using the stamper algorithm. The quality of the image which is recovered will be best while compared with the existing scheme.

Keywords: Extended visual cryptography scheme, Meaningless shares, Visual secret sharing schemes, Pixel expansion, Stamping algorithm, GAS solver.

1. INTRODUCTION

In accordance of ensuring the integrity, availability and the confidentiality of the transmission of the data which has been shared across the Internet, the normal traditional cryptography uses the key which is secret and tedious computation in order to convert the plain text which is original to the meaningless cipher text in order to share the secrets securely. The greatest drawback in this system is that it includes the process of encryption and decryption, which results in the high execution time and the computation resources, gets wasted. A visual secret sharing scheme was first introduced by the Naor and Shamir [3], in which it is called the visual cryptography (VC), in which it includes the process of encoding a ciphered secret image into *n* noise like divisional parts. In the prevailing system, the GAS Solver will take care of estimate the number of shares and the partition of the pixels among the users as appropriate shares. This system will react differently based on the number of partitioned shares and integration of different number of shares involved in the system and the contents of the image will be taken by an automatic decipher concept amend with de-wrapping on the stamping layer. To avoid complication on the shares due to noise in the share and lack of clarity on the image this process is used. This new Visual Extended cryptography scheme incorporates a known image on the share to distinctly identify the share. Additional advantages of this proposed system includes the detection of the shares by the synthesizer. In addition, this option will overcome pixel growth too. The step of pasting or stamping an image over the image is the second step in the process. The demerits

[1,3] Dept of Information Technology, *Emails: robertmtech2005@gmail.com, jbshaarul@gmail.com*

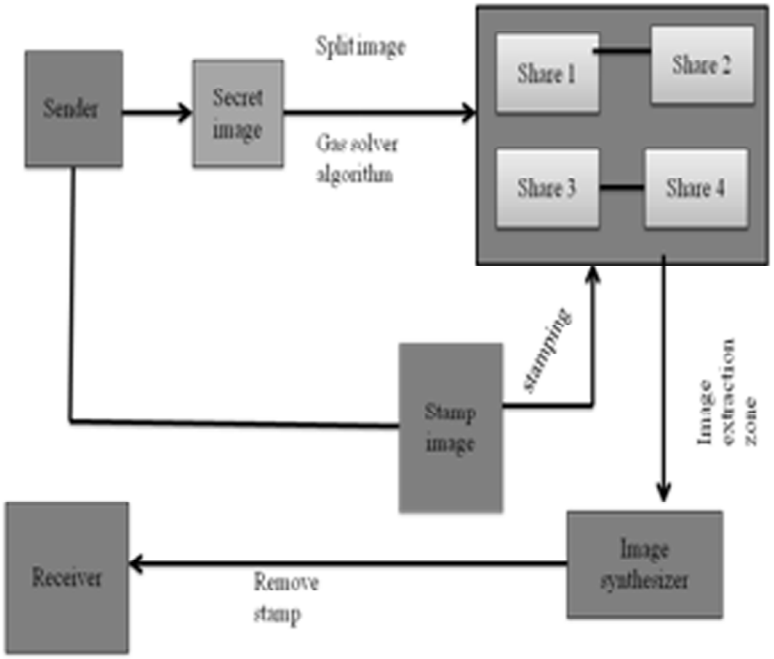
[2] Department of Physics Vel Tech MultiTech Dr.Rangarajan Dr. Sakunthala Engineering College, *Email: celinearuldoss@gmail.com*

in the existing system can be overcome by enhancing the quality and clarity of visualizing image before processing into the system. There is no assurance that the secret share has received the authorized receiver. The proposed system involves an automatic segregator which segregates images automatically which is a process of converting any images in two steps into Visual cryptographic formatted images. The partitioned image share appears in a random way which contains no decipherable data about the secret visual share.

This paper includes a cover image which then needs to be encoded into N number of shares printed on each partition. The choice of providing the resolution for the number of shares specified by the user is the advanced feature introduced. Once the shares were considered, the shares need to be stamped with the help of "Block-Based Ciphered-Transformation Algorithm". Now a detailed picture of image segregation must be undergone based on the viewable identifiers which can be used further. Enhancing clarity and quality of the image before processing the shares and after stamping the image using the algorithm is a most important feature which yields an added advantage while extracting the image and deciphering it to make to be a normal image. This paper also involves two step processes which contains the process of removing the cover image and de-ciphers the logic in each share and the following process will be decided based on the access structure [4]. The image which is being processed will be stored in the database, in which after getting the correct image, the images will be divided into number of shares depending on the access structure hierarchically [5]. This paper has the major advantages such considering colored images for this Visual Cryptography, the shares were stored in the DB repository for future references, storing the shares in a safe repository, and Microsoft's latest concept of storing the data in the format of File Stream in the database is used in this system. One of the major advantages of this system is enhance the clarity of the image before considering for processing it.

2. SYSTEM MODEL

The user will be with a secured login and the choices in accordance with providing all the needed information. Multi-users can be created in an hierarchical structure so that the data owner will login in to the system in which then an automatic bifurcation of images will take place based on the logged in user's sub childs. The data about the hierarchy must be feed into the GAS system. Logging of the users into this security system is enabled with the algorithmic security of MD5. Then the process proceeds with the uploading of images into the system in turn the automatic recognizer of GAS will then analyze the general access structure



inside the system and in which as the result, the images will be divided and then preceded for the following process. In this visual cryptography scheme [6] each pixel 'p' selected from the secret image is encrypted and converted into cipher as a pair of sub pixels. If the pixel 'p' is considered to be white then, one of the two columns under the white pixel is selected and if 'p' is considered to be black then, one of the two columns under the white pixel is selected. In both the cases, the selection of the pixels is performed in a random way in which each column has the probability of 50% to be chosen.

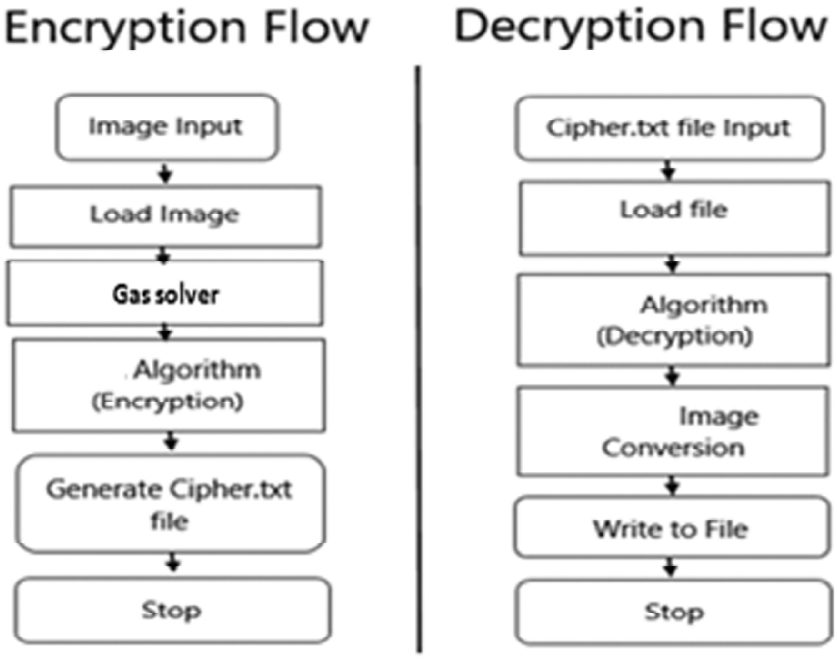
The above points are applicable for an system which contains only two shares whereas in our system, the GAS solver will take care of identifying the share numbers in an automatic way. Depending on the share counts, the pixel will be further divided and it's ready to be shared with the end user. The drawback of the existing system is that we do not have a proper system to identify such kind of images. To overcome these problems, the stamping system is involved in this system.

This image stamping system involves pasting a meaningful share on top of the partitioned share. This is a complex part involved in this system. Once the images were provided by the user of the system, the images were considered for the further validation. An automatic image synthesizer system will take care of validating the images and it will be merged. In case, the images were not in a good shape or not an appropriate one, an automatic indication of the image not available will be given to the system. Once the images were fed into the system normally, the images will get combined based upon the white pixel and black pixel combination which the final images will be re-constructed. Now the process of removal of stamp is done and the de-ciphering logic behind the share and get synthesized based on the access structure. Now the original image gets retrieved securely in the receiver side with much improvement in the quality.

3. ALGORITHM FOR THE PROPOSED SCHEME

3.1. Block Based Ciphered Algorithm

The image can be divided into units called blocks. Each of the blocks has specific number of pixels. Then these blocks are transformed into new determined locations.The block size should be small in order to make the transformation better, because few pixels alone will keep their neighbor pixels. The correlation will be decreased as the result and thus it becomes very difficult to find the value of given pixel from the neighbors values. The original image can be obtained by the inverse transformation of the blocks at the receiver side.



3.2. Visual Binary Algorithm

The encoding of image into n number of shares and the message can reveal by embedding k of those n shares. However, if k-1 shares are embedded together, the resulting encoded message cannot be visualized to the user.

A share generation scheme corresponding to n = 2. This can be applied only to a binary image by considering the corresponding sub pixel which has been grouped to the pixels throughout the image. This results in random image of two shares where the message cannot be revealed. In reference with this algorithm this proposed system was done.

4. RELATED WORKS

4.1. Two Secret Sharing Schemes Based on Boolean Operations

The traditional way of sharing the secret schemes involve complex manipulation and computation. A visual secret sharing (VSS) scheme includes decoding of the visual secrets without any computation, but each distortion based shadow in the secret is l times as big as the original. The Probabilistic VSS has solved the complex computation and space complexity problems at the same time. In this paper, the probabilistic (2, n) scheme[7] has been proposed for binary images and a deterministic (n, n) scheme adaption for grayscale images is done. Both uses the simple boolean operations and together does not suffer pixel expansion problem. The (2, n) scheme yield a satisfying contrast and smaller recognized areas than the other traditional methods. The (n, n) scheme yields an exact reconstruction of the share. It not guarantees that every black (resp., white) pixel of the original image will be coded as black (resp., white) in the resultant image recovered.

5. CONSTRUCTIONS AND PROPERTIES OF K OUT OF N VISUAL SECRET SHARING SCHEMES

The explicit constructions for k = 2 and k = n can be identified for general k out of n schemes bounds described. Here, two general k out of n constructions were produced and their parameters were relating maximum size arcs or MDS codes[8]. Further, analysis results on the structure of k out of n schemes were identified, and bounds on the parameters, were obtained. At last, the notation of the colored visual secret sharing schemes and a general construction is also introduced.

6. A GENERAL FORMULA OF THE (T; N)-THRESHOLD VISUAL SECRET SHARING SCHEME

This paper yields an advantageous method for construction of generating matrices of the (t; n) threshold visual secret sharing scheme[9] ((t; n)-VSSS)) for any n ¸ 2 and 2 • t • n. This shows that there is a bisection exists between a set of generating matrices of the (t; n) VSSS and in a set of homogeneous polynomials of the degree n which satisfies certain property and also shows that the set of homogeneous polynomials is identified with the set of lattice points in an linear space of dimension n ¡ t + 1 with expressed bases and in turn these results produces a general formula of the generating matrices of the (t; n)-VSSS. This formula is not only theoretically interest, but also enables us to obtain efficient generating matrices. This approach cannot be applied to the cases especially in 6 • t • n ¡ 2.

7. VISUALCRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES

This paper provides a combinational steganography[10] and cryptography concepts for the strongest visual secure systems. The added advantage in this proposed scheme is the zero truncation. The ciphered text is then retrieved by obtaining the difference in the pixel value from the closest predefined value and these numbers will now able to define the saved bit and which will form the ciphered text. The truncation of the

multimedia content of this paper is one of the major demerits. This paper also emphasizes on the usage of jpeg file and it remains an remarkable drawback in case of using different types of images. This paper also does not discuss the major impact of using other type of images.

8. GOAL-PROGRAMMING-ASSISTED VISUAL CRYPTOGRAPHY METHOD WITH UNEXPANDED SHADOW IMAGES FOR GENERAL ACCESS STRUCTURES

This paper gives the detailed information about a visual cryptography method in consideration with the elimination of pixel expansion and the improvements of contrast of the image are achieved. The proposed scheme uses a probabilistic concept of constructing multi objective linear programming model for general access structures and then, the solution space of the model explored by the goal programming [11]. The merits of the proposed method are fourfold. Foremost, the expanding of the shadow images is avoided. Secondly, contrast of the image can be reached better. Third, the desired contrast levels in each of the cases can be achieved using the general access structure. Fourth, it can be easily used to deal with the problems of many secret images. Experiments on many access structures shows that this proposed method is effective against pixel expansion and it is capable of improving the contrast.

9. ANALYSIS OF OUR ALGORITHM

In this two step secret sharing schemes sharing the visual securely is done based on the Boolean operations which we have referred that the concept of using the XOR operation in which the pixel expansion problem is avoided to a greater extends.

In the general formula of the (t; n)-threshold visual secret sharing scheme [12] we have referred the concept in which based on the threshold the secret sharing gets operated.

In the Region Incrementing Visual Cryptography [13] we have referred the concept of partitioning based on the regions of the secret share by detecting the secrecy levels.

10. EXPERIMENTAL WORK AND RESULT:

Protecting the secret is an alarming issue in the distributed systems. Henceforth, my concept of visual allocation of image stamper synthesizing technique can be used as a sound solution to construct privacy preserved image transfer and access control concepts in organizations, where the data owner can partition the image based on the designation of the partners. Users can obtain the secret share from the data owner and using the block based ciphered algorithm the removal of the stamping is done. As a result, our scheme can provide the following important properties: 1.Provides an automatic segregation which can be take place on the images which involves the process of conversion of the images into needed visual cryptographic formatted images; 2. After extracting the exact visual secret image, the images will be bifurcated into number of shares which depends on the hierarchical access structure; 3. The two step process of removing the stamp and de-ciphering the logic behind the share will be determined by the access structure which is already defined.

11. TEST AND RESULTS

This extended visual cryptography schemes takes the image as input in which it plays an important role throughout the system. The control flow includes the image to be shared secretly without any distortion in the quality Fig. 1 shows the various secret image which are given as input to the system.

Considering fig 1(d) for this experimental test, by applying the GAS solver algorithm, the secret image is getting partitioned based on the partition count specified, for example let me consider count = 4. So the resultant output for this GAS Solver algorithm will be shown in Fig. 2

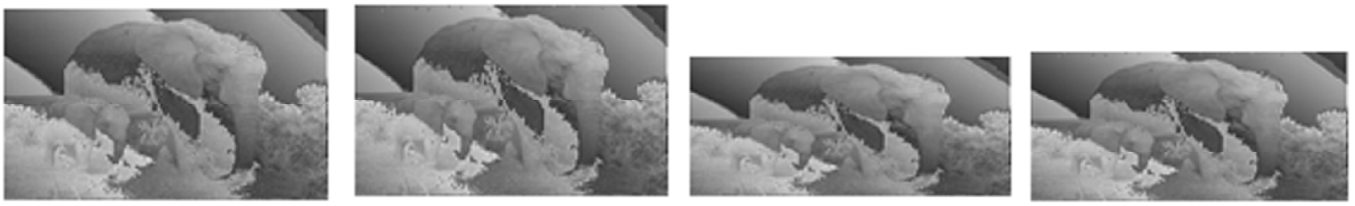
Considering image (a) and (b) in Fig:3 the resultant output for the Image Stamper Algorithm will be as in the Figure 4.

As the result in the Extended visual cryptography scheme all input image gets converted into single bitmap image format and gets into the process of GAS solver and the Image stamping process. Finally

(a) **(b)** **(c)** **(d)** **(e)**

(f) **(g)** **(h)** **(i)** **(j)**

Figure: 1



(a) **(b)** **(c)** **(d)**

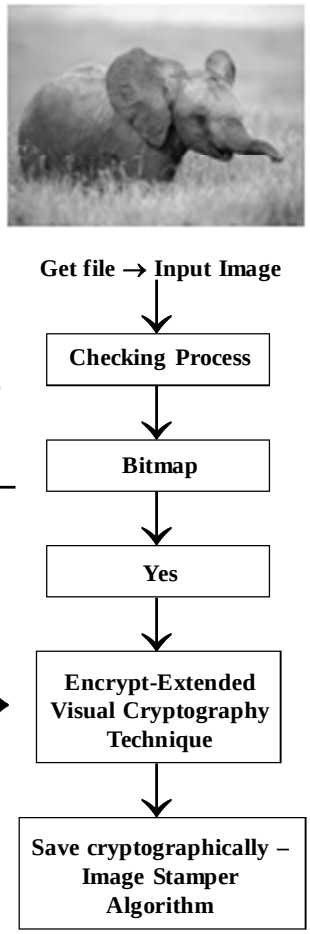
Figure: 2

(a) **(b)** **(c)** **(d)**

Figure: 3

(a) **(b)** **(c)** **(d)**

Figure: 4



the original secret image is retrieved without any distortion in the pixels, colour contrast, quality and size.

This above flowchart describes the visual cryptographic process involved in this system. So, the inverse process yields the original secret image in the receiver side.

12. SUMMARIES AND FURTHER EXTENSION

Stamping process can be done through designated levels so that stamping and removal of stamping process will gets increased so as to make the visual secret sharing more effective.

13. CONCLUSION

The performance and security analyses was made efficient to securely manage the image in the secret sharing system. Image partitioning is done using the GAS solver and made effective through the access structure. Pixel expansion problem, contrast modification, quality loss and image size variation are strictly avoided through this system.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the contribution of Govt. of India for Financial Assistance, DST-FIST F.NO:SR/FST/College-189/2013

REFERENCES

[1] Hao-Kuan Tso, “Secret Sharing Using Meaningful Images”, Department of Computer Sciences and Communication Engineering, Army Academy R.O.C., Chungli, Taoyuan 320, Taiwan, Journal of Advanced Management Science, Vol. 1, No. 1, March 2013.

[2] Y. C. Hou and J. H. Wu, "An Extended Visual Cryptography scheme for concealing cover images", in proc, 5th conf. Inform. Manage. Police Administ. Prac., 2001, pp. 62-69 (in Chinese).

[3] M. Naor and A. Shamir, "Visual Cryptography", in proc. Adv. Cryptology-EUROCRYPT'94, LNCS 950, 1995, pp. 1-12.

[4] K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Tran. Inf. Forensics Security, Vol. 7, no. 1, pp. 219-229, Feb. 2012.

[5] Feng Liu, Wei Qi Yan, "Visual Cryptography for Image Processing and Security Theory, Methods, and Applications.

[6] Youmaran. R, Adler. A., Miri. A., "An Improved Visual Cryptography Scheme for Secret Hiding", Communications, 2006 23rd Biennal Symposium, 340-343.

[7] Lei Zhang, Ning Ma, Xiaobo Li, "Pattern Recognition", Vol 40, Issue 10, pp. 2776-2785.

[8] Eric R. Verheul, Henk C.A. Van Tilborg, "Design, Codes and Cryptography", May 1997, Vol 11, Issue 2, pp. 179-196.

[9] Hiroki Koga, "Advances in Cryptography-ASIACRYPT 2002", Vol. 2501, 2002, pp. 328-345.

[10] Marwaha P., "Computing Communication and Networking Technologies (ICCCNT), 2010, pp. 1-6.

[11] Ching-Sheng Hsu, Young Chang Hou, "Image Processing", Vol. 45, Issue 9.

[12] Carlo Blundo, Paolo D. Arco, Alfredo De Santis, and Douglas R. Stinson, April 24, 1998.

[13] Ran-Zan Wang, "Region Incrementing Visual Cryptography", IEEE Signal Processing Letters, Vol. 16, No. 8, August 2009.