A New Visual Cryptography Approach using Mosaic and Spread Spectrum Watermarking

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

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

ABSTRACT
Visual cryptography is a furtive distribution scheme where a screte image is encrypted into the shares which independently make known no information concerning the secret original image. The attractiveness of the visual surreptitious distribution method is its decryption progression i.e. to decrypt the surreptitious image using human visual scheme be deficient to any calculation or no need of any computational devices. By using this special characteristic property anyone doesn't need any type of computational devices to recognize the secret image during the decryption process, VC is suited to be used in the environment which has no computational device. There are many researchers who have faithful themselves to study the related issues of Visual Cryptography because of its special property. The existing methodology implemented for the Representation of Visual Cryptography Algorithms is on the basis of efficient encryption of Images as compared to other encryption procedures such as AES, DES etc.

Here an efficient technique is implemented by using the combinatorial method of mosiacing the image and then applying spread spectrum for the water marking of secrete information thrashing and applying an effective cryptography algorithm.

Keywords
Visual Cryptography, Mosaic Images, Spread Spectrum Technique, Watermarking, Stenography

1. INTRODUCTION
With the development in digital media, the requirement of methods for protection such information is necessary. The source of digital media's growth can be linked to the wealth of information provided by the Internet. Every day the information downloaded and uploaded increases in the form of simple text documents to photos of individuals to hyper-spectral image cubes of the world. The use of internet is the way to access that knowledge. There is a need to protect that information.

Visual Cryptography field has been evolved over the last several years. The first method was suggested by Naor and Shamir [1] for binary images. This provides a entirely secure system where secret messages are enclosed in "shares". Independently these shares simulate random noise, but when they are arranged and aligned properly, their secret message is decrypted by only the human visual system. This method provides security for the text and binary images, then development of digital media need the step-up of this technique to provide security to the gray and color images. CryptOgraphic Algorithms visuaL simulAtion – COALA is an ideal graphical system presented. This system is developed for responding level of participation [2], in this system users are giving answers to questions concerning the visualization presented by the system. Previously our people were at the no viewing engagement level, since no visualization tool was used. In order to contain high interactivity [3], this sytem was developed to enable users to control the execution of algorithms forward and backward, it allows them to configure the parameters of algorithm before starting an execution, and it makes it possible for them to follow the result of every operation in any time. Security already exists and to define which characteristics should such system have in order to be successfully used as an educational aid. It was observed that there is only a small number of systems that can be used for visual representation of cryptographic algorithm and none of these systems fully covers the needs of the Data Security essence. Based on the systematization of the existing systems for visual representation of algorithms with special attention on those that can be used for visual representation of cryptographic algorithms a methodology for the development of such system is proposed. By analysis of the literature that is concerned with the eLearning tools an efficient way of using the developed system in education process is defined. The developed system enables detailed analysis of the execution of all cryptographic algorithms. It presents all details of the execution of supported algorithms, where it is significant for understanding the system works with real world lengths of the algorithm parameters, and all input parameters in the algorithms are configurable in order to make it possible to easily and quickly show execution of algorithms on different examples. This feature guarantee that this method can be performed by anyone who has no prior knowledge of Visual Cryptography, cryptographic analysis or programming background. To the developmentment of this idea, many different variations and modifications have been developed to explore many various views of VC (Visual Cryptography). Algorithm visualization tools have been used in the education process for a long time and a lot of different tools have been created [2]. Some of these are described in a survey paper focusing on program visualization and algorithm animation systems [4]. For classify these tools on the basis of their learning outcomes, survey is used to find that the interaction between students and a visualization system is more essential than the visualization contents [5].

As a part of the dissertation, some reviews were given : an overview of the eLearning tools field, an overview of the field covering systems for visual representation of algorithms (AV systems), and an overview of the field concerned with systems for visual representation of cryptographic algorithms. The description of cryptographic algorithms that are supported in the COALA system is presented. The system supports five different types of cryptographic algorithms: substitution algorithms (Caesar,

monoalphabetic, Playfair, and Vigenere algorithms), transposition algorithms (Rail Fence and Row Transposition algorithms), production algorithms (Rotor Machine), symmetric block algorithms (DES and AES), and public-key algorithms (RSA). Special focus is placed on the explaination about the visual representation used in the COALA system.

2. LITERATURE SURVEY

In this paper [6], here author have explained the novel COALA system for visual representation of the cryptographic algorithms, and experiences from using it at the Data Security course taught at the SEE-UB. The software system is designed to support the laboratory exercises which cover complex cryptography algorithms like: DES, AES, RSA and Diffie-Hellman that are taught in the course. To the best of our knowledge this is the first implementation of the AES algorithm in a learning supporting tool. Also, it describe other mentioned algorithms, COALA contains the possibility to walk users through the whole algorithm execution step-by-step that are using real world examples. The functional description of the system and several key design and implementation details are presented in the paper.

The most important objective of the beginning of the COALA system in the Data Security course was to help students to better recognize the algorithms taught in the course and to help them prepare for the exam. Numerical indicators show [6] that the percentage of the students who accepted the exam and the standard grade on the assessments for the duration of one school year increased for the students who used the COALA system. Results of measurements shown that the introduction of the COALA system brought benefit to all users, especially to those users who previously could not pass the exam in the first examination period of a school year and to some of the best students to improve their grades.

One of the approaches to keep a secret safe is secret sharing. VC is the well-known approach if the secret is an image. Most of the studies discuss the concept of visual cryptography for binary images. Later on, Visual Cryptography was extended for Gray Scale Images. Another visual cryptography scheme is (k, n)-threshold scheme. This scheme was described by Naor and Shamir. In this, a secret image is encoded into n shadow images that are also called shares. Recovering secret image involves stacking any k of the n shares but if k-1 or less stacking shares are there then no information about the secret image can be revealed[7].

In [8] interactive visualization applets are presented for cryptography.These algorithms used some tools for: Simple Substitution Cipher, Affine Cipher, Shift Cipher , Vigenere Cipher, RSA Cipher, RC4 Stream Cipher, and DES Cipher. This interface allows users to input the text which is to be encrypted and key. Some interactively control analysis tools such as frequency graphs, key length analysis, and diagram maps are provided. In this, DES Cipher process has two rounds of a Feistel system with textual description of operations peroformed in one round, and it interactively moves bits through the diagram to shows data movement in the algorithm.

DES Visual [9] is a visualization tool for the DES algorithm. It represents execution of IP (initial permutation) and first round of the DES algorithm in visual format. 8 or 16 bits input and 6 or 10 bits key are used in this method shown as a diagram. It has operations in two modes: trace mode and guided encryption/decryption mode. In trace mode the tool executes all operations and users can follow a specific bit across operations by clicking on it. In the next mode (guided encryption /decryption), the tool go ahead through each operation and asks users to calculate the result of a current operation.

In [10] , A Visual Information (pictures, text, etc.) is allowed by Visual cryptography technique to be encrypted in such that decryption becomes such a mechanical operation for which there is no requirement of a computer. There is splitting of original image into shares and it can't be possible for unauthorized person to get the data which is hidden within that share images. The secret data can be revealed just by stacking the two shares. Similarity in quality and size of the reconstructed image from the original image is the highlighted issue in VC. In this, in order to improve security and to produce meaningful shares, a novel k out of k extended visual cryptography scheme (EVCS) is used. In halftone visual cryptography (VC), there is an encoding of a secret image into k halftone meaningful image shares through error diffusion algorithm of Floyd steinberg.

In [11], In existing methods, there is a work for color images with 8 colors and even few of them are without halftone techniques.

In this paper, a method is proposed for images with 256 colors and these are further converted to 16 standard RGB colors format. Shares are generated without compromising the resolution. The dithering algorithm of Floyd – Steinberg is used for the manipulation of the 256 color code image so as to reduce it to 16 standard colors code image. (2, 2) XOR-Based visual cryptography method employed by the proposed method is also used to generate shares. Secret image sharing and stacking is enabled by the Decryption procedure.

In the proposed scheme, a color secret image is decomposed into three shares. The secret image cannot be revealed by an individual share alone. However, if we gather any two of the three shares then secret image can be unveiled. In [12], A technique for protecting sensitive data is secret sharing , such as cryptographic keys. Literature is full of well-known secret sharing schemes such as Shamir, Asmuth-Bloom and Blakley which leads to high computational complexity during both sharing and reconstruction and also noise like shares are generated . In order to create meaningful shares, a method was proposed by Lin and Tsai that uses Steganography using the secret sharing scheme of Shamir and again that led to high computational complexity. There is a scheme that can overcome above problem and also deploys simple graphical masking method. generation, a simple ANDing is done and for reconstruction, a simple ORing is done on the qualified set of shares. Finally, the meaningful shares are created by using Steganography instead of noise like shares.

In [13], In visual cryptography methods, there is no boundation of randomness on color images. There are two basic process : Error diffusion and pixel synchronization. The Error diffusion in which there is filtering of quantization error at each pixel level and is further put as the input to the next pixel. In this, low frequency received between the input and output image is minimized which results in quality images. Color degradation is avoided with the help of pixel synchronization. In our proposal, we have generated an efficient color image visual cryptic filtering scheme for improving the image quality on restored original image from visual cryptic shares. An effect known as Deblurring effect,

which is presented by the proposed color image visual cryptic filtering scheme. This mechanism is applied on non-uniform distribution of visual cryptic share pixels. After the elimination of blurring effects on the pixels, there is need to apply fourier transformation to normalize the unevenly transformed share pixels on the original restored image. As a result, the quality of restored visual cryptographic image is improved to its optimal point.

3. PROPOSED METHODOLOGY

The Planned Practice implemented here is based on the concept of mosiacing the images and watermark using Spread Spectrum watermarking.

3.1 Proposed Algorithm

Spread Spectrum Watermarking

1. Take input Watermark and Cover image and a secrete image.
2. Choose alpha value which denoted watermark signal strength factor in spread spectrum algorithm, here in our work we assume alpha=0.5;
4. (Alpha value should be between 0 and 1.If the is less than 0.5, the watermark image will be less visible and if the alpha is more than 0.5, the watermark image will be clearly visible. The optimized value of alpha is 0.5)
3. Calculate DWT of the original image which is used for the transformation of the image to be embedded.
4. Calculate total number of pixels of the original image and watermark image.
5. Divide the water mark image into finite numbers of shares by using Masaic Technique.
5. (Here I have choose the share size 150 X 150 px.)
6. Calculate aj=bj where ir<=j<(i+1)r.
7. Calculate watermark signal as wj=alpha*aj*pj, where pj= {+1,-1}.
8. Now we will find the kernel of the image by taking kernel size 31 and by taking the level of the kernel size as 3 we will find the kernel image of the original image by calculating kernel image = (1/(2*pi*s^2))*exp(-((X-m).^2 + (Y-m).^2)/(2*s^2));
9. This watermark signal is then embedded with the kernel image to get the final watermark image.

The embedding process is carried out by first generating the watermark signal W by using watermark information bits, chip rate and PN sequence. The watermark information bits b= {bi}, where bi = {1,-1} are spread by r, which gives

$$Aj=bj \text{ , } ir<=j<(i+1)r$$

The sequence aj is then multiplied by alpha and P. The watermark signal W= {wj},where $wj=\alpha a_i P$,

Where, pj= {1,-1} the watermark signal generated is added to the encrypted signal, to give the watermarked signal Cw.

$$C_w = C + W = c_{wi} = c_i + w_i, \quad \forall_i = 0,1, \dots \dots \dots, L-1$$

The encrypted value of M2 denoted by C2 is

$$c_{2i} = (m_{2i} + k_{2i}) \, mod \, 255 \;\; \forall_i = 0,1, \dots \dots \dots, L-1$$

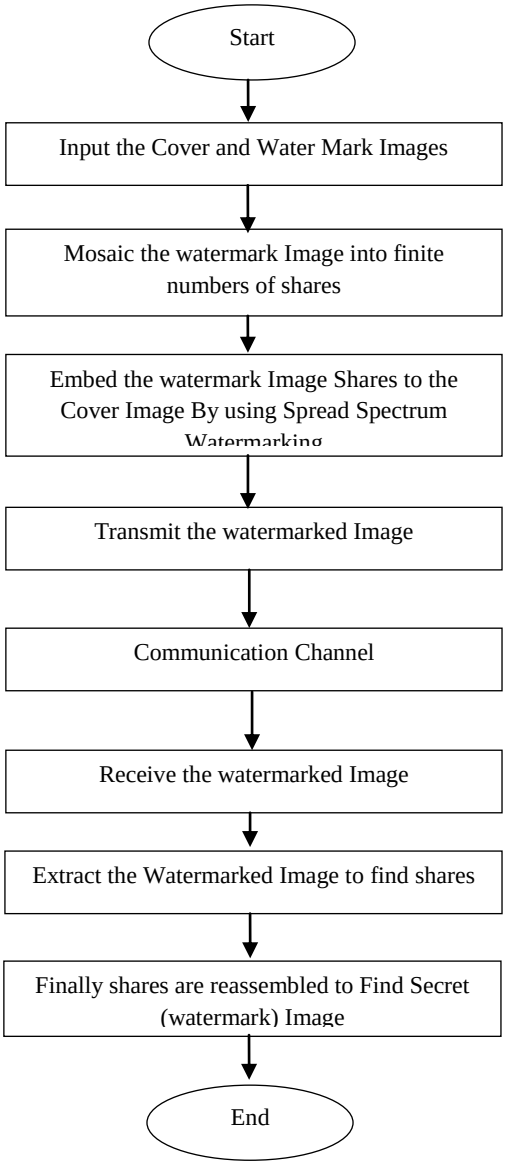

Figure 1. Flow chart of Spread Spectrum Watermarking

10. RESULT ANALYSIS

The Figure shown below is the mosaic images on the basis of Input Image on which encryption are to be performed. The Input image selected is divided on the basis of size of the input image and hence on the basis mosaic images are formed.

S N	Algorithm	No of Rounds	Size of keys	MSE	PSNR
1	AES	14	64	0.5600	45
2	DES	16	48	0.3400	56
3	RSA	1	1024	0.1200	79
4	PROPOSED	1	0	0.1000	82

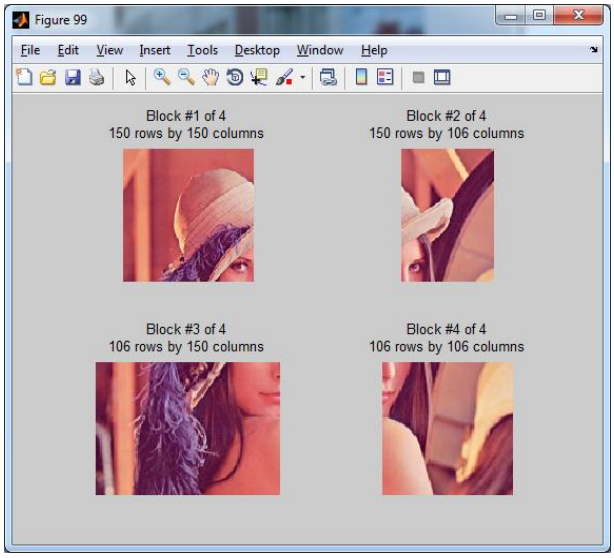

Figure 2 Mosiac Images using Proposed Methodology

The Figure shown below is the analysis and comparison of various Visual Cryptography techniques. The proposed methodology implemented here for Visual Cryptography provides less no. of rounds for the operations to perform.

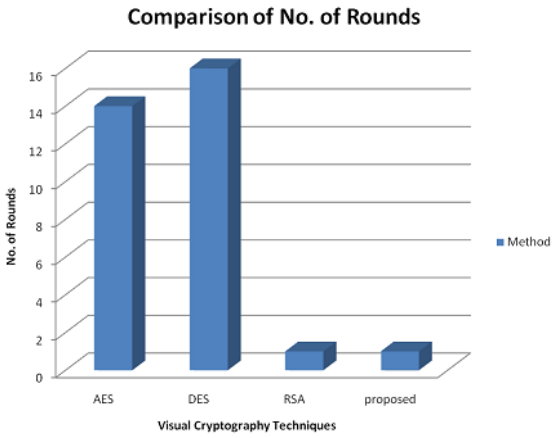

Figure 3. Comparison of No. of Rounds

The Figure shown below is the analysis and comparison of various Visual Cryptography techniques. The proposed methodology implemented here for Visual Cryptography provides less size of keys for the operations to perform.

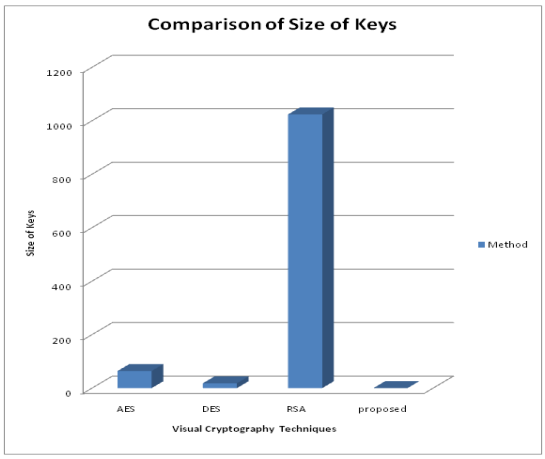

Figure 4. Comparison of Size of Keys

The Figure shown below is the analysis and comparison of various Visual Cryptography techniques. The proposed methodology implemented here for Visual Cryptography provides less Mean Square Error for the operations to perform.

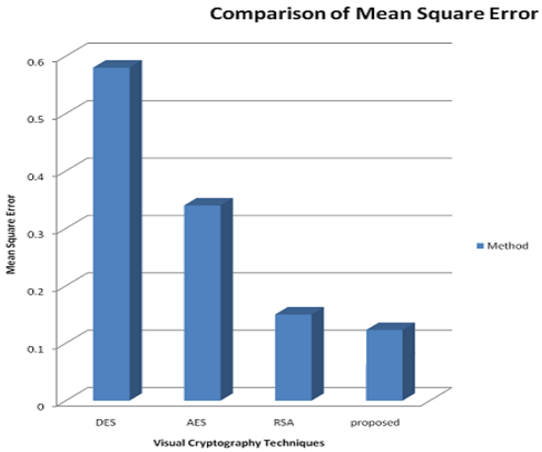

Figure 6. Comparison of Mean Square Error

The Figure shown below is the analysis and comparison of various Visual Cryptography techniques. The proposed methodology implemented here for Visual Cryptography provides high Peak Signal to Noise Ratio for the operations to perform.

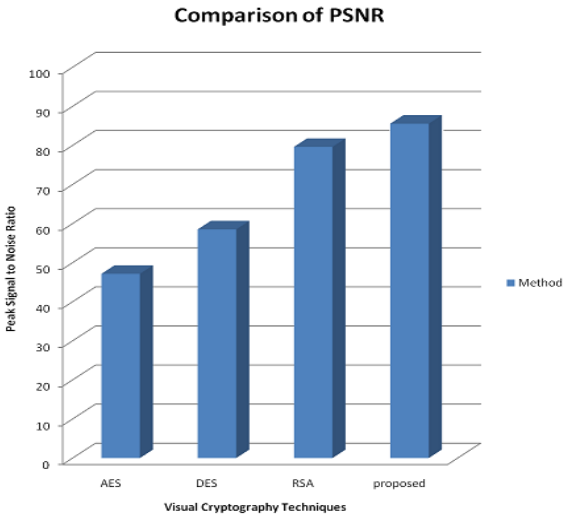

Figure 5. Comparison of PSNR

11. CONCLUSION

The Proposed Methodology applied here for the Visual Cryptography uses the concept of mosaic images and then watermarking that images using Spread Spectrum Watermarking. The methodology adopted here takes less error rate as well take less storage space as well zero rounds to perform the operations.

Although the proposed methodology implemented here is feasible for the Steganography but there are future enhancement done in the technique such as image stenography of HDR Imaging, low computational time and less iteration and complexity should be minimized.

12. REFERENCES

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

[2] J. Urquiza-Fuentes and J.A. Ve azquez-Iturbide, "A survey of successful evaluations of program visualization and algorithm animation systems," ACM Trans. Comput. Educ., vol. 9, no. 2, article 9, pp. 1–24, Jun. 2009.

[3] D. Schweitzer and W. Brown, "Interactive visualization for the active learning classroom," ACM SIGCSE Bull., vol. 39, no. 1, pp. 208–212, Mar. 2007.

[4] C. A. Shaffer,M. L. Cooper, A. J. D. Alon,M. Akbar,M. Stewart, S. Ponce, and S. H. Edwards, "Algorithm visualization: The state of the field," ACM Trans. Comput. Educ., vol. 10, no. 3, article 9, pp. 1–22, Aug. 2010.

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

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

[7] Kun-Yuan Chao, Ja-Chen Lin,"(2, 3)-threshold visual cryptography for color images", Proc. of the 6th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision, Elounda, Greece, August 21-23, 2006 (pp89-94).

[8] D. Schweitzer and L. Baird, "The design and use of interactive visualization applets for teaching ciphers," in Proc. IEEE Inf. AssuranceWorkshop, Jun. 2006, pp. 69–75.

[9] J. Tao, J. Ma, J. Mayo, C. K. Shene, and M. Keranen, "DESvisual: A visualization tool for the DES cipher," J. Comput. Sci. Colleges, vol. 27, no. 1, pp. 81–89, 2011.

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

[11] M.Karolin, Dr.T.Meyyapan,"RGB based secret sharing scheme in color visual cryptography",International Journal of Advanced Research in Computer and Communication Engineering, ISSN : 2278-1021,Vol. 4, Issue 7, July 2015.

[12] Prabir Kr. Naskar, Ayan Chaudhuri, Atal Chaudhuri," Image Secret Sharing Scheme Using a Novel Secret Sharing Technique with Steganography", IEEE CASCOM , pp 62-65, Nov. 27, 2010.

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