An Efficient Approach for Visual Cryptography Using Hybrid Mosiac image based SS

Asmita Mishra
Department of Computer Science & Engineering
Bhabha engineering and research institute
Bhopal, (M.P.)
mishraasmita0210@gmail.com

Dr. Tripti Arjariya
Department of Computer Science & Engineering
Bhabha engineering and research institute
Bhopal, (M.P.)
tripti.beri@gmail.com

Abstract—Here in this paper a new and efficient approach for the Visual Cryptography is implemented and is compared with other existing Visual Cryptographic techniques such as AES, DES and RSA. The proposed methodology implemented here is based on the concept of mosiacking the images and then encrypt each of the mosaic image into some cover image so that the secrete image is made hidden. The proposed methodology implemented takes less error rate as well as takes no storage space since the concept is independent of Keys.

Index Terms—Visual Cryptography, AES, DES, RSA, Deffie-Hellman, Mosiac Images.

I. Introduction

With the enhancement of digital media, the requirement for techniques to keep such data is becoming more essential. The source of digital media's expansion can be bonded to the prosperity of data make available by the Internet. The amount of data that is downloaded and uploaded enhances day by day, with data ranging from easy text documents to photos of entities to hyper-spectral image cubes of the world. The Internet provides an effortlessness of right of entry that requires information of the finest method to defend the visual data available on the Internet from stealing, replication, or unauthorized access, privacy protection, secure data communication, remote authentication and proof of ownership are well-known examples of digital security methods.

Visual Cryptography is a special encryption technique to hide information in images in such an approach that it can be decrypted by the human vision if the correct key image is utilized. Visual Cryptography uses two visible images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The field of Visual Cryptography has progressed steadily over the past several years. It initiated as a procedure to encrypt binary images to cover up messages controlling text and has evolved into encrypting color images as significant distributes to hide messages ranging from binary text to other color images. Visual Cryptography allows messages to be contained in seemingly random shares. The generation of these shares shows the idea of Visual Cryptography along with its powers and drawbacks.

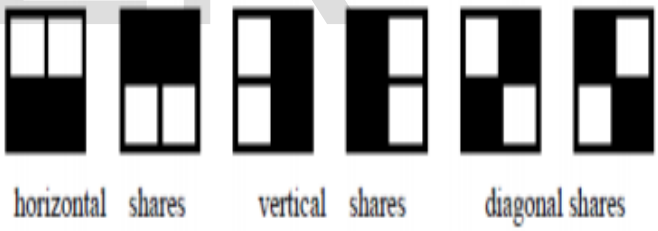


Figure 2.1: Shares Most Commonly Used for Visual Cryptography Algorithms [1]

Assuming that the message being encrypted is a binary image with p pixels, each of these pixels is individually encoded with a subpixel grouping with s pixels. This allows n shares to be generated using these subpixel groupings. Each distribute is a set of m black and white subpixels, which are printed in secure proximity to each other so that the human visual system standards their entity black/white contributions." [1] These subpixel groupings are typically square (s/2 x s/2) to not distort the aspect ratio of the original image. However, subpixel groupings that are not square do occur in Visual Cryptography algorithms and the characteristic relation of the image is modified consequently.

As this area persists to develop and increase in its competence, a standard process is helpful to emphasize the strong points and limitations of each algorithm in addition to expansion regions that have not been met by the present algorithms. The most important explanation connected with Visual Cryptography is the message being encoded into two splits. When give the impression of being at independently, these distributes make known no data about the message controlled in them and look like random noise. On the other hand, when these splits are printed on transparencies, superimposed and completely supported the message contained in the splits is making known. The message is exposed without supplementary computation or exploitation. This characteristic promises that the protected procedure can be utilized by an important person who has no earlier information of Visual Cryptography, programming conditions, or cryptographic investigation understanding. Since the expansion of this design, numerous dissimilar discrepancies and alterations have been enlarged to investigate many different characteristics of Visual Cryptography. Some of these incorporate an algorithm for encrypting precise image regions [2]. In 1994, Naor and Shamir [1] proposed a rising cryptography technique that is to say, visual cryptography (VC), which is very simple to make use of that and entirely secure. The encryption process is completed by easy and low computational mechanism, but the decryption process is executed straightforwardly by human visual system without any composite computations. Visual Cryptography can be utilized where computers are inadequate or right of entry to them is not achievable [3, 16-17]. Visual cryptography separates a secret image into n transparent splits and it utilizes the human visual system to get better the secret image by superimposing and supporting with awareness all or some of n transparent distributes according to visual cryptography method used [3].

.

II. Literature Survey

In this paper here author [6] have explained the new CryptOgraphic ALgorithm visuAl representation (COALA) scheme for visual representation of the cryptographic algorithms and knowledge's from using it at the Data Security course taught at the SEE-UB was to facilitate students to better recognize the algorithms taught in the course and to help them get ready for the exam.. This method is proposed to sustain the laboratory exercises which cover difficult cryptography algorithms like: DES, AES, RSA and Diffie-Hellman. To the most excellent of our information this is the initial implementation of the AES algorithm in a learning sustaining device. Also, contrasting other subsisting devices which explain other declare algorithms. Numerical indicators show that the percentage of the students who passed the exam and the average grade on the exams during one school year enhanced for the students who used the COALA [6] system. Results of amounts give you an idea about that the COALA method brought profit to all students, in particular to those students who earlier could not pass the exam in the first examination period of a school year and to some of the best students to get better their grades.

In this paper [7] a set of interactive visualization applets for teaching cryptography algorithms is presented. Here author has compared with various algorithms covered by this tool are: Shift Cipher, Simple Substitution Cipher, Affine Cipher, Vigenere Cipher, RC4 Stream Cipher, RSA Cipher, and DES Cipher. The interface allows clients to input the text to be encrypted and the key and to interactively manage investigation tools for example: frequency graphs, key length analysis and diagram maps. Here they use applet for DES Cipher give you an idea about two rounds of a Feistel system as a diagram with textual explanation of operations in a round and it interactively shifts bits through the diagram to demonstrate data flow in the algorithm.

Grasp [8] is a visualization tool for teaching security protocols. It can be arranged by a customer to visualize any security protocol (e.g., Diffie-Hellman), since it make available protocol measurement language that permits an arbitrary number of actors and message passing with suitable commands required for security protocols. Users can edit protocol commands during the visualization permitting them to scrutinize "what-if" circumstances and they can manage the protocol implementation by moving a step forward or backward, resetting or terminating the execution.

In this paper [9], Chaotic Pseudo –Random Number generation, Zigzag Scan Pattern technique, to decrease the degradation of the consequential image is proposed by an expansion from gray to colour image. These might include Military Secrets, Commercial Secrets and data of individuals and therefore it has to be transmitted by securer means with improved safety measures. Pixel Index technique is conversed to get betters the safety measures for images. The Secret whose text format focused to encryption using substitution cipher and the consequential encrypted text were embedded into the image. When they distributes on transparencies are superimposed precisely together the unique secret can be determined without computer contribution. As using this technique security enhances as the scrambling is additional. Here author [9] proposal aspires at Visual cryptography which make available a very dominant method by which one secret can be distributed into two or more pieces known as distributes. Experimental Analysis shows that their time consumption is also in terms of Nano seconds and therefore this technique can be applicable in most of the application domain and the problem of pixel expansion is also eliminated.

In this paper, N. Askari e.t.al proposed [10] a new method based on extended Visual Cryptography method with preprocessing halftone images' two techniques Simple Block Replacement (SBR) and Balanced Block Replacement (BBR). Here they using simple approach and extremely efficient for unprocessed binary secret images which have large number of all white and black blocks these are some advantages of this SBR and BBR methods. The Balanced Block Replacement method employs the idea of candidate block 'CB' which consists of block of two white and two

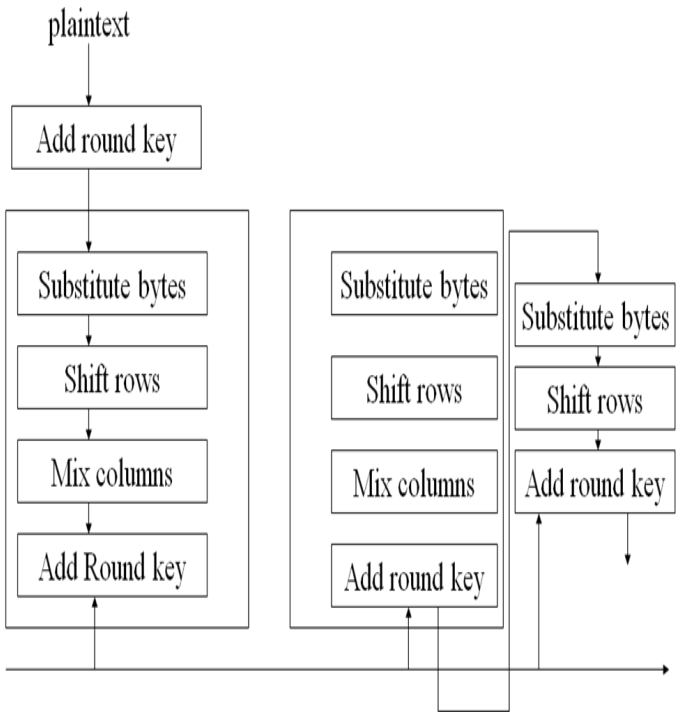
black pixels. It progress the visual quality of the developmental image. The BBR method tries to continue the local ratio of black to white pixels in the processed image close to the local ratio of black to white pixels in the original halftone secret image. The algorithm used for BBR method is as follows: a) the secret image is processed into halftone picture, b) split the image into four have common characteristics clusters each restraining four secret block, c) compute no. of black pixels for each cluster and save in a template, d) leaving only black, white or candidate block other blocks are converted into black pixels, e) turned the candidate block into black or white block, based on the minimum difference among the threshold and no. of black pixels, f) Repeat the step (e) for remaining clusters and get the final processed image.

Mainly existing system endures a management problem, because of which dealers cannot visually recognize each distribution. This difficulty is resolved by the Extended Visual Cryptography scheme (EVCS) [11]. Here author talk about the properties of the extended matrix collection for EVCS. Then they propose an EVCS for single color images with optimal extended matrix collection. The earlier methods for binary or grayscale or color images using random-looking contribute to can be straight expanded to produce above suspicion-looking contribute to using EVCS with bit-plane encoding method which make available the more safety measures over network. On the other hand, the existing system concerning the EVCS for common access structures suffer from a low contrast difficulty. Here, In this paper proposes a new (k,n)-threshold image sharing method using extended visual cryptography method for color images based on bit plane encoding that encrypts a color image in such a technique that consequences of encryption is in the form of shares. Shares do not replicate any information straightforwardly; information is scrambled as an alternative. The conventional binary EVCS is used to get the distribution images at every bit level of each standard module of a color image. This method gives a more proficient method to conceal natural images in different shares. Besides, the size of the hidden secret can be improved by examining the blocks in the shares. This novel method for color images gives the perfect contrast in the recovered image easily recognized and managed.

III. Proposed Methodology

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

AES Algorithm




```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
  Begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[0, Nb-1])
    for round=1 to Nr-1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
    end for
    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1)
    Out = state
  end
```

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
  Begin
    byte state[4,Nb]
    state = in
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1)
    for round=1 to Nr-1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[round*Nb, round+1)*Nb-1])
      InvMixColumns(state)
    end for
```

```
        InvShiftRows(state)
        InvSubBytes(state)
        AddRoundKey(state, w[0, Nb-1])
        Out = state
    end
```

Proposed Algorithm

Spread Spectrum Watermarking

1. Take an input 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=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. Calculate aj=bj where ir<=j<(i+1)r.
6. Calculate watermark signal as wj=alpha*aj*pj, where pj= {+1,-1}.
7. 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));
8. 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

$$a_j = b_i, \qquad ir \leq j < (i+1)r$$

The sequence aj is then multiplied by alpha>0 and P. The watermark signal W= {wj},where

$$w_j = \alpha a_j P_j$$

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

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

The encrypted value of M2 denoted by C2 is

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

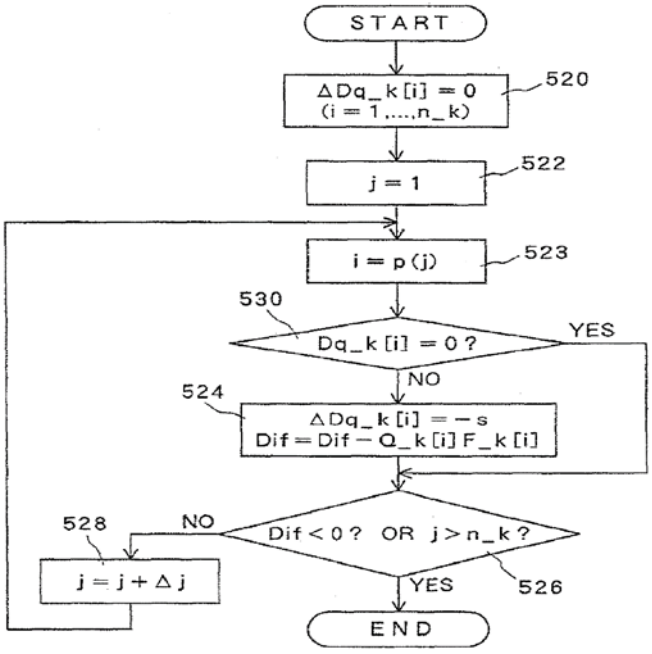


Figure 1. Flow chart of Spread Spectrum Watermarking

IV. Result Analysis

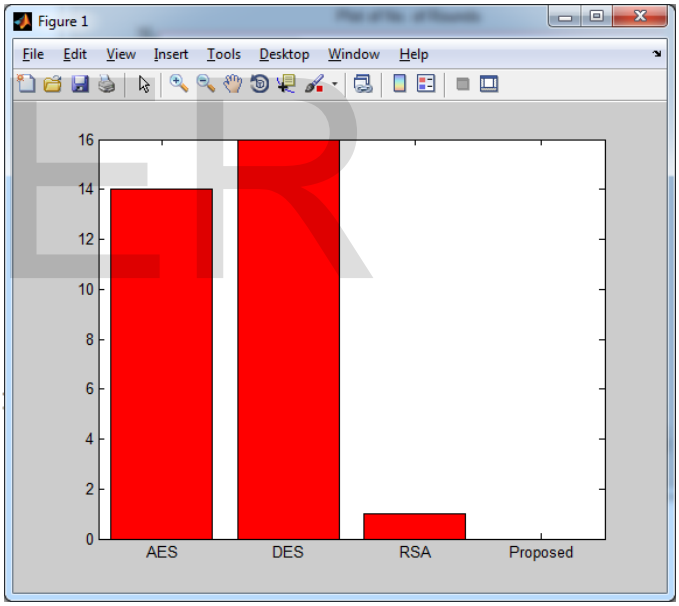


Figure 2. No. of Rounds Performed in Various Algorithms

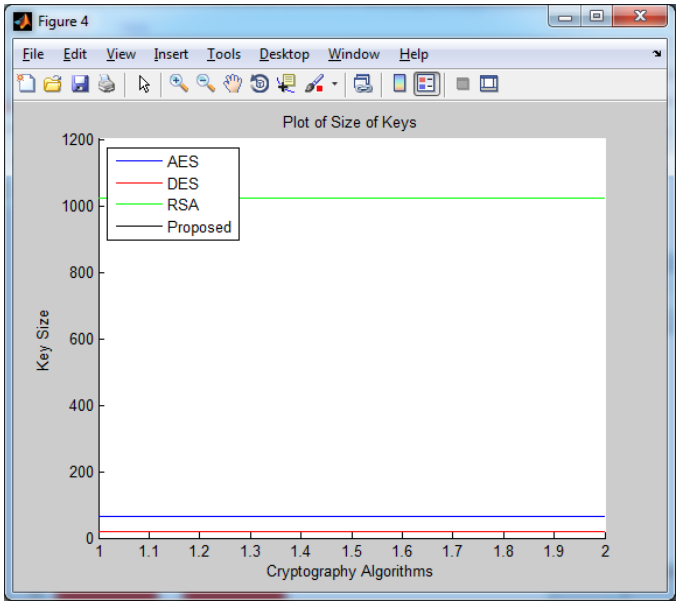


Figure 3. Size of Keys in Various Algorithms

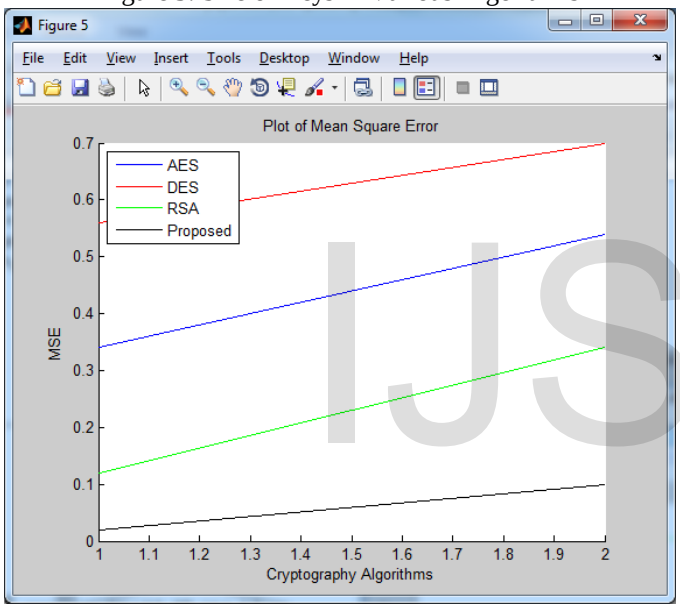


Figure 4. Mean Square Error of Various Algorithms

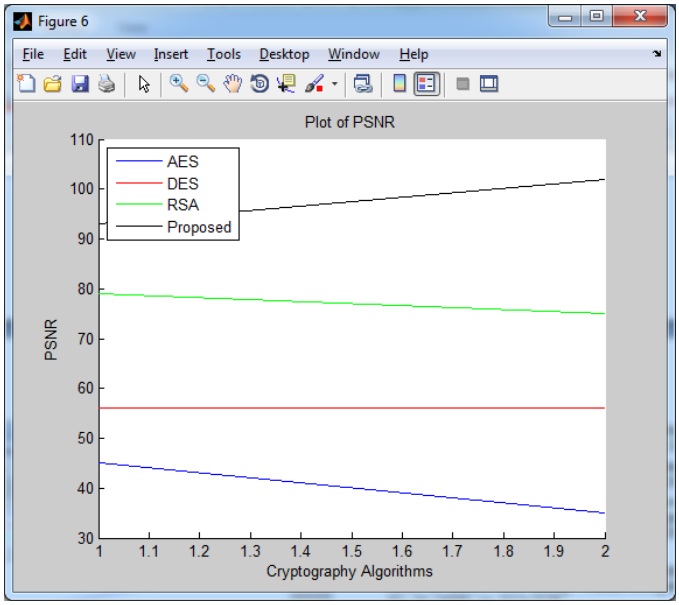


Figure 5. PSNR of Various Algorithms

V. Conclusion

The Proposed Methodology applied here for the Visual Cryptography uses the concept of mosaic images and then watermarking the mosaic 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.

References

[1] M. Naor, and A. Shamir, "Visual cryptography", Advances in Cryptology-EUROCRYPT'94, lecture Notes in Computer Science, Vol. 950, Springer-Verlag, Berlin, (1995), pp. 1-12.

[2] Ran-Zan Wang. Region incrementing visual cryptography. IEEE Signal Processing Letters, 16(8):659-662, August 2009.

[3] Y. C. Hou, "Visual cryptography for color images", Pattern Recognition, Vol. 36, No. 7, (2003), pp. 1619-1629.

[4] D. Tsai, T. Chen, and G. Horng, "A cheating prevention scheme for binary visual cryptography with homogeneous secret images", Pattern Recognition, Vol. 40, No. 8, (2007), pp. 2356-2366.

[5] C. Yang, and T. Chen, "Colored visual cryptography scheme based on additive color mixing", Pattern Recognition, Vol. 41, No. 10, (2008), pp. 3114-3129.

[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] 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.

[8] D. Schweitzer, L. Baird, M. Collins, W. Brown, and M. Sherman, "GRASP: A visualization tool for teaching security protocols," in Proc. 10th Colloquium Inf. Syst. Security Educ., Jun. 2006, pp. 75–81.

[9] Krishna Kumari & ShashiYadav, "A New Procedure of Visual Cryptography for Maintaining the Security of Visual Information Transaction using Java Based Approach"

International Journal of Research (IJR) Vol-1, Issue-9, October 2014.

[10] N. Askari, H.M. Heys, and C.R. Moloney "An extended visual cryptography scheme without pixel expansion for halftone images", 26th IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) 978-1-4799-0033, 2013.

[11] Arti, Pushpendra K Rajput, "An EVCS for Color Images with Real Size Image Recovery and Ideal Contrast Using Bit Plane Encoding" .I. J. Computer Network and Information Security, 2014, 2, 54-60.