I.J. Image, Graphics and Signal Processing, **2013, 6, 49-56**
Published Online May 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2013.06.07

A Novel Visual Cryptographic Method for Color Images

Devinder Kumar, Amarjot Singh
National Institute of Technology,Warangal
devinderkumar@ieee.org, amarjotsingh@ieee.org

S.N. Omkar
Indian Institute of Science, Bangalore.
omkar@aero.iisc.ernet.in

Abstract— Visual cryptography is considered to be a vital technique for hiding visual data from intruders. Because of its importance, it finds applications in various sectors such as E-voting system, financial documents and copyright protections etc. A number of methods have been proposed in past for encrypting color images such as color decomposition, contrast manipulation, polynomial method, using the difference in color intensity values in a color image etc. The major flaws with most of the earlier proposed methods is the complexity encountered during the implementation of the methods on a wide scale basis, the problem of random pixilation and insertion of noise in encrypted images. This paper presents a simple and highly resistant algorithm for visual cryptography to be performed on color images. The main advantage of the proposed cryptographic algorithm is the robustness and low computational cost with structure simplicity. The proposed algorithm outperformed the conventional methods when tested over sample images proven using key analysis, SSIM and histogram analysis tests. In addition, the proposed method overshadows the standard method in terms of the signal to noise ratio obtained for the encrypted image, which is much better than the SNR value obtained using the standard method. The paper also makes a worst case analysis for the SNR values for both the methods.

Index Terms— Visual cryptography, Color images, Computational Cost, SSIM, Histogram Analysis

I. INTRODUCTION

Visual cryptography [1] was introduced as a technique allowing the visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be carried out by human visual system, without the aid of computers. Due to the immense importance of encryption algorithms, visual cryptography find applications in various sectors such as E-voting [2] for giving encrypted receipts, in financial documents for encrypting sensitive financial data[3], copyright protections [3] etc. The present systems are mainly used to protect sensitive data transferred over the internet like multimedia data, audio data etc. Due to the confidential information related to the applications, there is immediate need to have stronger and robust systems for transferring the vital and confidential data over various kind of network safely. These encrypting technologies encrypt the data i.e. make it distorted/unrecognizable based on a pattern or using a key which later can be recovered through the use of correct/same key.

A number of algorithms have been proposed in the past to secure the data. In 1994, Moni Naor and Adi Shamir [4] introduced the term Visual Cryptography algorithm (VCS) that presented a simple yet a secure way to share secret information with cryptographic computations. Since then many visual cryptography algorithms were presented mainly emphasizing on rendering the pixel values of the source image through one or other kind of operation. Some of the work done presented by Hou et al [5] used the color decomposition and contrast manipulation for encryption while the authors in [6] used the polynomial method for sharing the pixel values of the input image. In addition [7], attempts have also been made to obtain image encryption using the difference in color intensity values which is very effective method and yet requires minimum computation cost. The effectiveness of the algorithms above is evaluated using some of the standard tests including SSIM index test [8], statistical analysis [9], differential analysis [10] etc. The strength of any visual cryptographic algorithm can also be evaluated through its ability to encrypt different images w.r.t to original images with minimum noise insertion.

The methods proposed in past have many limitations. Most of the algorithms proposed in past resulted into insertion into the encrypted image [11] and require heavy computational requirements. In addition, the methods described have the problem of random pixel distribution [12]. The method proposed in the paper overcomes these limitations and presents a more secure method for data transmission.

In this paper, we propose a cryptographic algorithm which functions upon rendering the basic structure of the image by manipulating each individual pixel's value.

Due to operating and changing the source image at pixel level, the algorithm effectively encrypts the input image. The effectiveness of proposed algorithm is demonstrated by the tests carried out in the later section. Also, the decryption of image can be easily performed by just reversing the encryption steps (mentioned in the section 3) along with the key. The proposed algorithm overcomes the limitations of the previous method as (i) The resulting encrypted image has high signal to noise ratio (ii) It is computationally efficient hence it can be used over the internet and requires less resources (iii) It doesn't faces the problem of random pixel distribution as the pixel are distributed through a fixed formula accurately.

The following paper has been divided into five sections. The next section explains the standard method used for encryption of visual data. The third section elaborates the encryption algorithm proposed by the paper. Section four explains the simulation results while the final section puts forward the summary of the paper, explaining the significance of the results obtained through the experimentation.

II. STANDARD ALGORITHM

This section states the visual cryptography algorithm used to encrypt colored images [13] as show in fig. 1 (a). In the first step of the algorithm, color image and the two keys are given as input to the system along with the resizing factor r . Using the stated mathematical function

$$f(t) = abs(1/\log(\tan((\exp(a)*\cos(\exp(b))*\sin(\exp(O)))))) \quad (1)$$

the values for the encryption keys are obtained and stored. In the above equation a and b are the keys and O is the GCD of the two keys. In the next step, the absolute value of the function $f(t)$ is calculated and passed through the low pass filter. Further, bi-cubic interpolation is used to resize the image and the resulting RGB values are stored in a separate matrix along with the resizing factor r . In the next step, absolute value calculated previously is multiplied with the pixel values of the image. In the subsequent step, Red intensity component matrix is flipped 180 degree upside down while the green intensity component matrix 180 degree left-side right. After this, the blue intensity matrix is rotated two times the resizing factor r . Finally, the entire three intensity matrices are joined to form the encrypted image and saved in .bmp format.

III. PROPOSED ALGORITHM

This section states the proposed algorithm implemented in this paper as shown in fig. 1 (b). The algorithm is based on rendering the basic structure of a color image resulting into a complex encrypted image. In the first step of the algorithm, the image is given as input to the system. In the next step, the function

$$p(i, j) = \exp(\tanh(\log(\sinh(i1 + j1)))) \quad (2)$$

where i, j are the pixel co-ordinate & $i1, j1$ are the loop variables, generates random values for each iteration, collected to form the two dimensional random key matrix p . In the next step, the key matrix is multiplied with Red, Green & Blue component matrices of the input image. Further the new Red intensity matrix is flipped 180 degree from left to right; the Green matrix is flipped 180 degree from top to down and the Blue matrix is rotated by factor of 90 degrees. Lastly, combine the new manipulated individual R, G, B matrices to form the encrypted image. The algorithm stated above is used to encrypt the image while for the decryption process the key matrix is transferred as the deciphering Key which can be used by reversing the encryption process to obtain the original image.

IV. TESTS PERFORMED

This section explains the various test performed on the proposed algorithm to check the efficacy of algorithm. The tests performed are described below:

A. Key Structure Analysis Test

The key is of vital importance for the algorithm as both the encryption and decryption process cannot be completed without it. The proposed algorithm generates a key matrix of a very large size consisting of numerous values which can resist any brutal attack. We test the sensitivity of the algorithm against the key matrix by changing the objective function given in step 2 of the section 3. Four different objective functions were tested for this task:

1. $p(i, j) = 1/(\log(\cos(\exp(\sin(\log((\mathrm{i1+j1})\char`^2))))))$ (3)
2. $p(i, j) = (\tanh(\sec((\mathrm{i1+j1}))));$ (4)
3. $p(i, j) = \exp(\tanh(\log(\sinh(i1 + j1))))$ (5)
4. $p(i, j) = \exp((\tanh(\log(\sin(\mathrm{i1+j1})))))$ (6)

The results obtained from each of the individual function are presented in the paper.

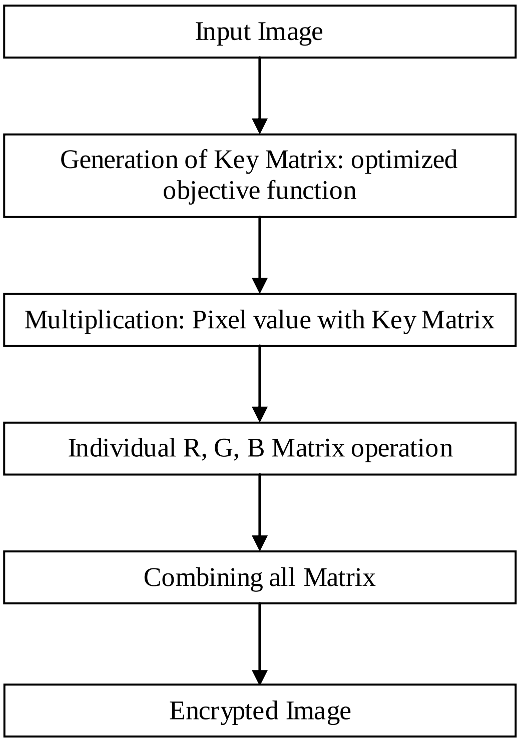
Input Image
Generation of Key Matrix: optimized objective function
Multiplication: Pixel value with Key Matrix
Individual R, G, B Matrix operation
Combining all Matrix
Encrypted Image

Fig 1(a) Flow chart for Standard Algorithm

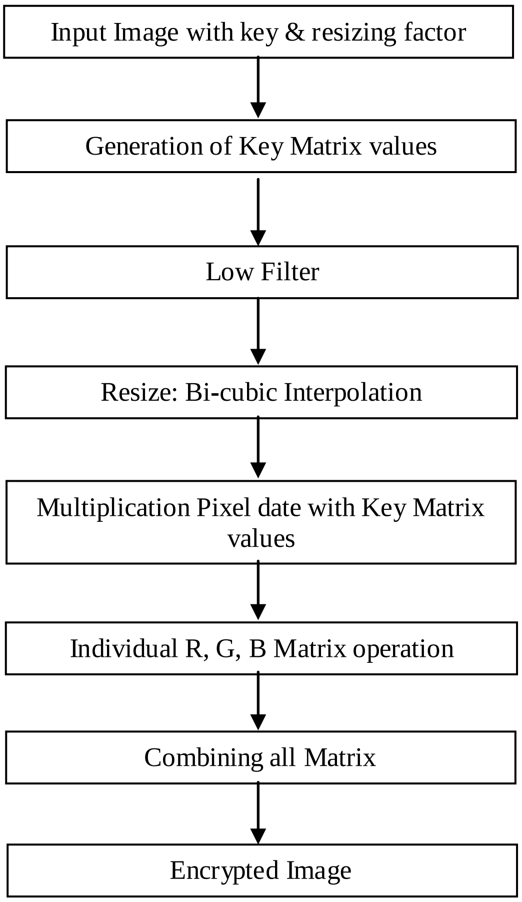
Input Image with key & resizing factor
Generation of Key Matrix values
Low Filter
Resize: Bi-cubic Interpolation
Multiplication Pixel date with Key Matrix values
Individual R, G, B Matrix operation
Combining all Matrix
Encrypted Image

Fig 1(b) Flow chart for Proposed Algorithm

B. Structure Similarity Index (SSIM) Test

This test is generally used to check the similarity between original and encrypted images. The robustness and efficiency of any cryptographic algorithm is established by the extent of similarity between the original and its encrypted image. The process of comparing the test image with original/source image gives a similarity index value. If the similarity index is small, there is a small similarity between the structure of encrypted and original image. The above statements prove that SSIM test can act as a viable way to test the efficacy of cryptographic algorithms. The SSIM test was performed on various images for all four different objective functions as stated in section 4 (a).

C. Statistical Analysis through Histogram Test

A prominent way of attack makes use of statistical nature to hack the real world encryption systems. Hence, it is advantageous if the encrypted image bears little or no statistical similarity with the original image.

In order to test the statistical similarity/dissimilarity, we perform histogram analysis for both the original image and encrypted image. The analysis illustrates the distribution of pixels for both original and encrypted images.

V. RESULTS

This section elaborates the results obtained from the experimentation performed using the proposed algorithm on three colored images. The aim of the experimentation is to test the effectiveness of the proposed algorithm against different kind of attacks and to compare the results with the previous method described in section 2. The simulations were carried out on the windows 7 platform using the Matlab R2007a release on 2.27 GHz core i3 processor machine. An average runtime of 1.2 seconds was recorded for the algorithm to encrypt the images.

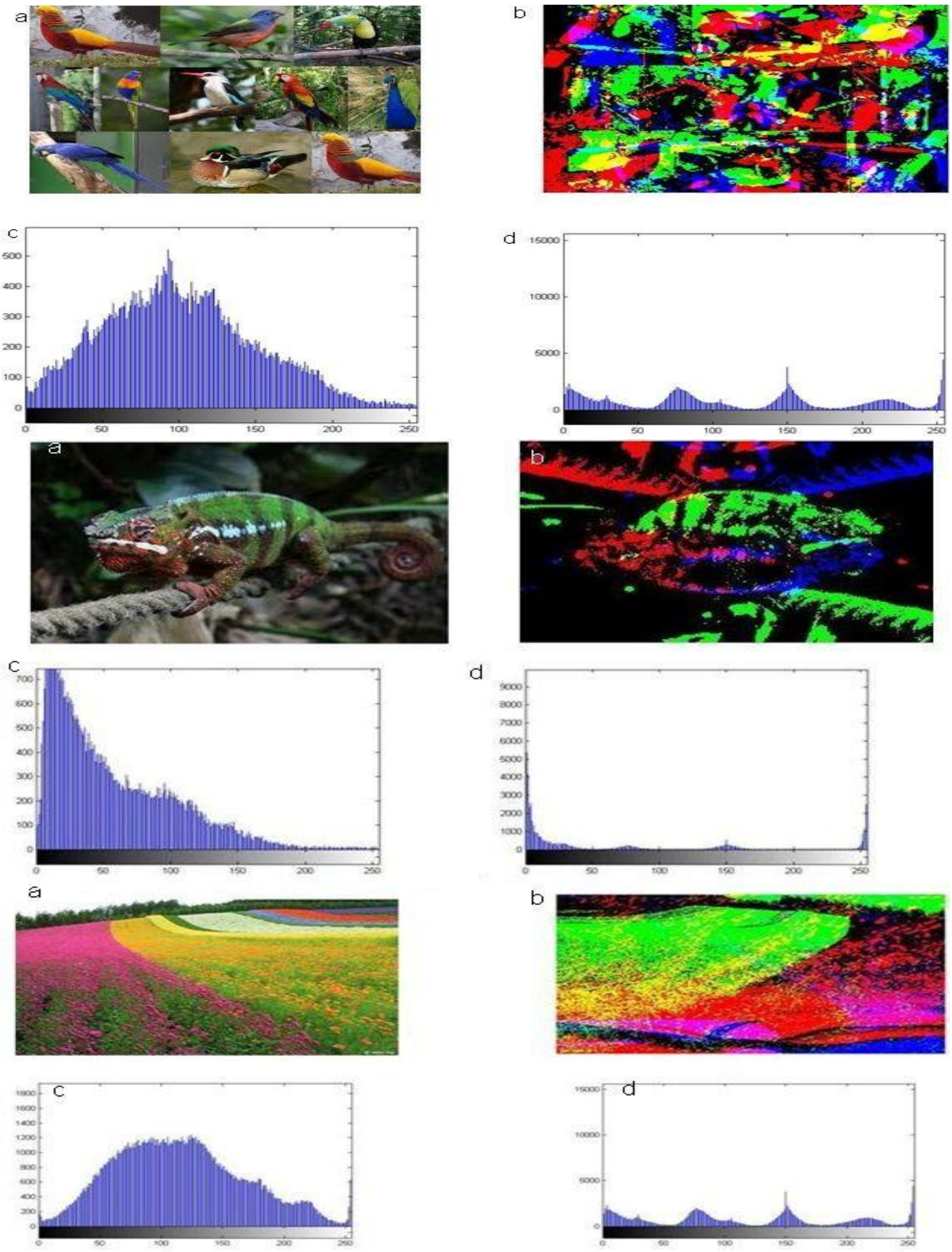

Fig 2 (a) Input image to the proposed algorithm (b) Encrypted Image for the input image (c) Histogram of the input image (d) Histogram of the encrypted image

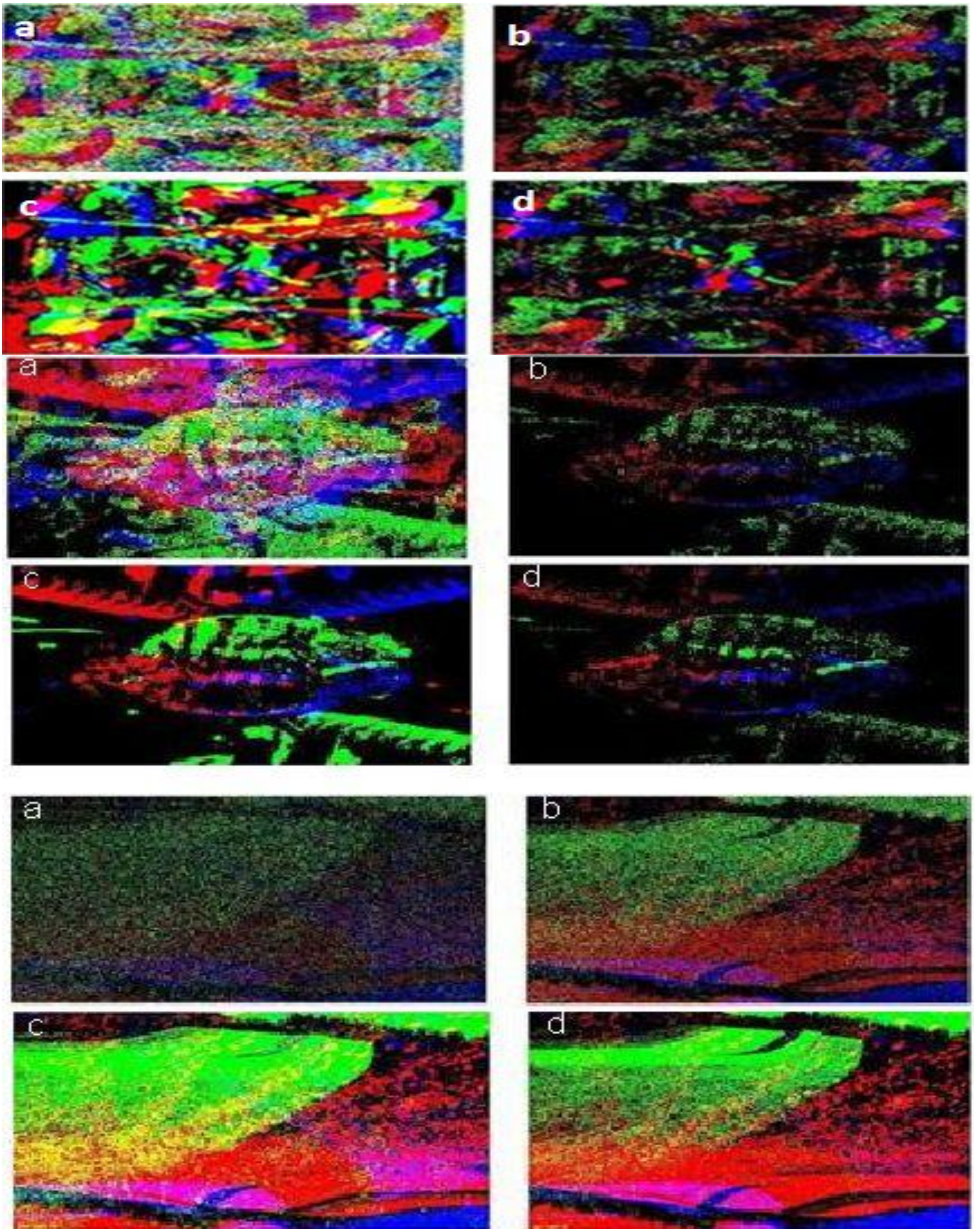

Fig 3 (a) Encrypted Image for objective function-1 (b) Encrypted Image for objective function-2 (c) Encrypted Image for objective function-3 (d) Encrypted Image for objective function-4

Table 1. Table representing the SSIM index test value for the images for all the objective functions respectively

Images	SSIM Index values			
	Obj. Function 1	Obj. Function 2	Obj. Function 3	Obj. Function 4
Images-1	0.000130	0.000193	0.000102	0.000112
Images-2	0.000142	0.000201	0.000119	0.000139
Images-3	0.000175	0.000212	0.000124	0.000177

Table 2. Table representing the SNR value for encrypted images for all the objective function respectively

Images	SNR (dB) (OF-1)	SNR (dB) (OF-2)	SNR (dB) (OF-3)	SNR (dB) (OF-4)
Images-1	3.08	3.78	2.94	2.98
Images-2	3.14	3.83	3.01	3.12
Images-3	3.80	4.12	3.04	3.81

Table 3. Table representing the SNRvalue for the encrypted images for all the objective functions respectively

Images	SNR (Standard Method) (dB)	SNR (Proposed Method-Best csase) (dB)	SNR (Proposed Method-Worst csase) (dB)
Images-1	2.33	3.78	2.94
Images-2	2.78	3.83	3.01
Images-3	2.94	4.12	3.04

For the Key Structure Analysis Test, four different objective functions were used and tested respectively for encrypting images as shown in fig. 3. Further to find out the best possible objective function SSIM test was performed on each encrypted image in order to obtain the most efficient objective function. The result of the SSIM test is shown in the Table 1. From the values in the table it is evident the objective function 3 generates the most efficient results. In order to test the efficiency of encryption for third objective function, we performed histogram analysis on encrypted images as show in fig. 2. The figure shows the histogram for the input and encrypted images. It is quite evident from the figures that the histogram of the input and encrypted images differ by a great margin from each other proving the high efficiency of encryption algorithm.

The efficiency of the proposed method is also proved using signal to noise ratio. The signal to noise ratio of the encrypted images obtained for all four objective functions is computed as shown in table. 2. Further, the comparison is performed for best and worst case signal to noise scenario for all four objective functions obtained using proposed method with the signal to noise obtained using standard method on input images as shown in table. 3.

VI. CONCLUSION

This section presents a brief summary of the paper. The key matrix, consisting of different combinations of secret keys or values makes the proposed algorithm more effective against all types of attacks. The results shown in table 1 for the SSIM index test are evidently very low indicating that the two images i.e. the original image and the encrypted image are very much different from each other for each of the objective function. This can be concluded as there is no way of obtaining or recognizing the visual data from the encrypted image which signifies the strength of the proposed algorithm towards the leakage of information to any unwanted person. The results in table (1) are better than obtained through the algorithm explained in section 2 (results of which are given in [2]).Also comparing individual results of the table it is evident that the third objective function is the most efficient of all. The results shown for the histogram analysis indicate that the intensity for different color levels in the encrypted images is totally different from the source images. In addition, it is observed that the worst signal to noise ratio value obtained for encryption on input image from the proposed algorithm is more than the best signal to noise ratio value obtained using the standard method proving the superiority of the proposed algorithm. Also, this depicts that proposed cryptographic algorithm has covered up or altered all the characteristics of the source image and complicated the dependence of statistics of output on the statistics of the input. This protects the algorithm from any kind of statistical attack therefore increasing the overall strength of the algorithm. On the other side the very small amount of time taken by the algorithm for generating the encrypted image or the output shows the low computational cost of the method. All these things make the proposed algorithm more favorable to be used in the practical modern day encryption systems to protect the visual data flowing in any kind of communication network. In future this system can be joined with any kind of data transfer mechanism that can enhance the overall data flow capability of the network

REFERENCES

[1] M.Naor and A Shamir, “Visual Cryptography”, Proceeding of Eurocrypt 94 Lecture Notes in Computer Science, LNCS963: Springer, 1994,

[2] D Chaum, “Secret-ballot receipts: True voter-variable elections”, *IEEE Security and Privacy*, pp 38-47, 2004

[3] W. Hawkes, A. Yasinsac, C. Cline, An Application of Visual Cryptography to Financial Documents,technical report TR001001, Florida State University (2000).

[4] P. S. Revenkar, Anisa Anjum, W. Z. Gandhare: Secure Iris Authentication Using Visual Cryptography International Journal of Computer Science and Information Security, Vol. 7, No.3, pp217-221 ,2010

[5] Y.C. Hou, C.Y. Chang, F. Lin, Visual cryptography for color images based on color decomposition, *Proceedings of the Fifth Conference on Information Management*, Taipei, November 1999, pp. 584–591.

[6] C.C. Thien and J.C. Lin, “Secret image sharing,” *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[7] Jing Dong; Tieniu Tan; "Effects of watermarking on iris recognition performance" 10th International Conference on Control, Automation, Robotics and Vision, 2008. ICARCV 2008.

[8] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600-612, Apr. 2004.

[9] Alfredo Rizzi, “Statistical Methods for Cryptography” Proceedings of the 6th Conference of the Classification and Data Analysis, 1st Edition., 2010, XXII, 482 p. 109 illus.

[10] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” Lecture Notes in Computer Science: Advances in Cryptology-Proceedings of CRYPTO ’90, Springer-Verlag, 1990, pp. 2- 21.

[11] An Application of Visual Cryptography To Financial Documents L. Hawkes, A.Yasinsac and C. Cline, An Application of Visual Cryptography to Financial Documents; technical report TR001001, Florida State University (2000).

[12] R. Hwang, A digital Image Copyright Protection Scheme Based on Visual Cryptography, Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000)

[13] B.SaiChandana, S.Anuradha “A New Visual Cryptography Scheme for Color Images” in International Journal of Engineering Science and Technology,Vol. 2(6), 2010

Amarjot Singh is a Research Engineer with Tropical Marine Science Institute at National University of Singapore (NUS). He completed his Bachelors in Electrical and Electronics Engineering from National Institute of Technology Warangal. He is the recipient of Gold Medal for Excellence in research for Batch 2007-2011 of Electrical Department from National Institute of Technology Warangal. He has authored and co-authored 48 International Journal and Conference Publications. He holds the record in Asia Book of Records (India Book of Record Chapter) for having "Maximum Number (18) of International Research Publications by an Undergraduate Student". He has been awarded multiple prestigious fellowships over the years including the prestigious Gfar “Research Scholarship” for Excellence in Research from Gfar Research Germany and “Travel Fellowship” from Center for International Corporation in Science (CICS), India. He has also been recognized for his research at multiple international platforms and has been awarded 3rd position in IEEE Region 10 Paper Contest across Asia-Pacific Region and shortlisted as world finalist (Top 15) at IEEE President Change the World Competition. He is the founder and chairman of Illuminati, a potential research groups of students at National Institute of Technology Warangal (Well Known across a Number of Countries in Europe and Asia). He has worked with number of research organizations including INRIA-Sophia Antipolis (France), University of Bonn (Germany), Gfar Research (Germany), Twtbuck (India), Indian Institute of Technology Kanpur (India), Indian Institute of Science Bangalore (India) and Defense Research and Development Organization (DRDO), Hyderabad (India). His research interests involve Computer Vision, Computational Photography, Motion Tracking etc.

Devinder Kumar is an Undergraduate Student researcher currently pursuing his Bachelors in Electrical and Electronics Engineering at the National Institute of Technology Warangal. He is the one of the founding member & Co-ordinator of ILLUMINATI@NITW, a potential research group of students at National Institute of Technology Warangal

(Well Known across a Number of Countries in Europe and Asia).He is the Head of the Computer Vision & Image Processing Cluster at IEEE Student Branch NIT Warangal as well as a active member of IEEE, IEEE Communications Society and IEEE Power and Energy Society. His research interests mainly in the field of Computer vision ,Image processing & Machine learning in particular involving: Motion Tracking, Object Identification, Image Annotation.