A Keyless Approach to Image Encryption

Madhav Gupta , Dhruv Sethi , Kaustubh Parte, Anuj Redij
Department of Information Technology
Atharva College of Engineering, University of Mumbai, India.
{ madhavg91 , dhruvsethi22 , kaustubhsparte , anujredij }@gmail.com

Abstract **- Maintaining the secrecy and confidentiality of images is done by two different approaches , the first being encrypting the images using keys, the other approach involves dividing the image into random shares. Heavy computation cost and key management is a drawback of the first approach and the poor quality of the image limits the applications of the second approach. In this paper we suggest a different approach without the use of encryption keys. The approach employes Sieving, Division and Shuffling to generate random shares such that the computation time is reduced, the original secret image can be recovered from the random shares without any loss of image quality.**

Keywords **- *Visual Cryptography, Sieving, Shuffling, Random shares.***

I. INTRODUCTION

In cryptography, encryption is the process of encoding information in such a way that unwanted users cannot acess it. In an encryption scheme, the message to be protected is referred to as plaintext, is encrypted by an image encryption algorithm, converting it to a ciphertext . This is done with the use of an encryption key, which specifies how the message is to be encoded. Any party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption method, that will need a decryption key. An encryption scheme usually needs a key-generation algorithm to produce keys.

II. RELATED WORK

A. *Image Encryption*

Last few years has seen several methods proposed for image encryption using keys, A few of the prominent ones are. Manniccam and Bourbakis [3] in 1992 proposed an image encryption scheme using SCAN language but was applicable only to grey scale images. Similarly Xin and Chen [1] in 2008 following up on the work of [3], came up with a two stage encryption method.

B. *Image Splitting*

The method of Image splitting is referred to as Visual Cryptography Scheme (VCS) which involves splitting an image into n random shares such that these random shares will individually reveal no information . The random image shares are simply printed and stacked up revealing the original image. The issue with this technique is the poor quality of the image .

III. PROPOSED SYSYTEM

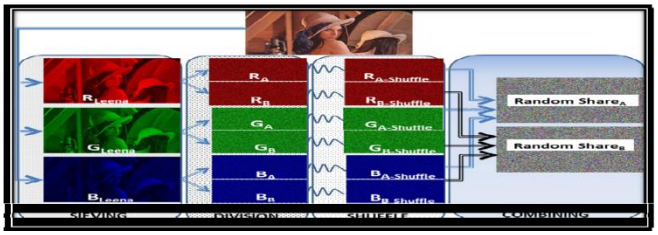
The technique involves splitting an image into no. of shares. The shares reveal no information about the secret image and to retrieve the secret image all shares are required. The technique is implemented with the SDS algorithm . In the first step the secret image is split into primary colors. In step two these split images are divided randomly. In step three these divided shares are then shuffled each within itself. Finally the shuffled shares are combined to generate the desired random shares. The process is shown in the below figure

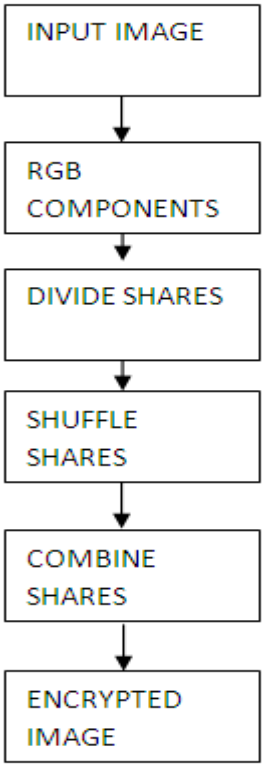
A. TABLE I. COMPARISON OF VISUAL CRYPTOGRAPHY SCHEMES

Authors Year	Pixel Expansion	Number of Secret	Image Format	Type of Share
Naor and Shamir [7]-	1	4	Binary	Random
Wu and Chang [9]	2	4	Binary	Random
Chin-Chen et. al [10] 2005	1	4	Binary	Meaningful
Tzung-Her Chen et al [11]	n(n>=2)	4	Binary, gray,	Random
F. Liu et al [12] 2008	1	1	Color	Random
Du-Shiau Tsai et al [13] 2009	1	9	Color	Meaningful

B. While representing colors, additive and the subtractive color models are preffered the most. In the RGB model, the three primary colors i.e. Red, Green, Blue are mixed to generate the desired colors. The colors as seen on the computers monitor are an example of the RGB model. Similarly while using the CMY model, the colors are represented by the degree of the light reflected by the colored objects.

C. As our techniques involves computation during the encryption and decryption of images and the results are to be viewed on the computer monitors therefore it is natural for us to use RGB model. The techniques based on [11], [12] in which the shares were printed on transparencies, hence CMY model was the obvious choice for such applications.





IV. METHODOLOGY

Sieving : Sieving involves filtering the combined RGB components into individual R, G and B components .Sieving depends on the range of values that R/G/B component takes individually. Sieving uses the XOR operator.

Division: After Sieving the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.

R (R_A, R_B, R_C,----------, R_Z)

G (G_A, G_B, G_C,----------, G_Z)

B (B_A, B_B, B_C,----------, B_Z)

Shuffling: This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of onethe other shares generated.

V. APPLICATION OF KEYLESS IMAGE ENCRYPTION

- For safety of critical images in several databases.
- Eg: Protecting Government images that are confidential.

VI. FUTURE SCOPE

The approach of Keyless image encryption saves on computation time which is very beneficial while dealing with large databases and with exponentially growing technology , the databases will become more complex.

VII. CONCLUSION

In this paper a new enhanced visual cryptographic scheme is presented, which is a hybrid of the traditional VCS and the conventional image encryption schemes. The proposed method has the following merits (a) The original secret

image can be retrieved in totality (b) Key management is not a issue.

Acknowledgment

This paper describes research done at Atharva College of Engineering in department of Information Technology. We express our gratitude to our project guide Mr. Sachin Gavhane for guiding us. We are eager and glad to express gratitude to Head of Dept. Prof Jyoti Chinchole and all the Project coordinators. We would like to deeply express our sincere gratitude to our respected principal Prof. Dr. Shrikanth kallurkar and the management of Atharva College of Engineering.

REFERENCES

[1] Xin Zhang and Weibin Chen, "A new chaotic algorithm for image encryption", International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.

[2] Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications(2003), 218(4-6), pp 229-234, online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]

[3] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), pp 1229-1245.

[4] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.

[5] S.Behnia,A.Akhshani,S.Ahadpour,H.Mahmodi,A. Akha-van, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,*Physics Letters* A 366(2007):391-396.

[6] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[7] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT' 94*, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[8] Arpad Incze, "Pixel sieve method for secret sharing & visual cryptography" RoEduNet IEEE International Conference Proceeding Sibiu 24-26 June 2010, ISSN 2068-1038, p. 89-96

[9] H.-C. Wu, C.-C. Chang, "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134 (28) ,pp. 123–135, (2005).

[10] Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin , "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005
.

[11] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.

[12] F. Liu1, C.K. Wu X.J. Lin , "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.

[13] Du-Shiau Tsai , Gwoboa Horng , Tzung-Her Chen , Yao-Te Huang , "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.

[14] R. Lukac, K.N. Plataniotis "Bit-level based secret sharing for image encryption", The Journal of Pattern Recognition Society, 2005.

[15] C.C. Chang, T.-X. Yu, Sharing a secret gray image in multiple images, in: Proceedings of First International Symposium on Cyber Worlds, 2002, pp. 230–
240.

[16] C.C. Thien, J.C. Lin, "Secret image sharing", Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770.

