IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

# Keyless Image Encryption using Hash Maps

**Anchal Monga[1*], Anubhooti Papola[2]**

[1*]Dept. of CSE, Uttarakhand Technical University, Dehradun , India
[2]Dept of CSE, Uttarakhand Technical University, Dehradun , India

[*]*Corresponding Author: anchal.anshu@gmail.com, Tel.:7017283448*

**Available online at: www.ijcseonline.org**

Received: 23/Feb//2018, Revised: 28/Feb2018, Accepted: 21/Mar/2018, Published: 30/Mar/2018

***Abstract*—** To develop the security, a new image encryption method that uses a keyless approach for image encryption is proposed. Keyless approach increases the ability of the system from various types of attacks as compared to the asymmetric keys that are vulnerable to various types of attacks. For security check of the system hash algorithms (MD5 and SHA128) are applied which checks whether the image transmission over the web is manipulated in between the transfer from sender to the receiver. The image is encrypted in such a way that it is not an easy task for the third party to recognize or create the original image by just seeing the encrypted image. Before the transfer of an image SHA128 and MD5 of the image is calculated. After the decryption of the image if SHA128 and MD5 of the system matches the image is not manipulated otherwise it is manipulated. So the Keyless approach, SHA128 and MD5 together increases the overall security of the system and make the system more secure by protecting it from different types of attacks. The outcome shows that the value of error matrix, PSNR is increased by approximately 8% and the values of MSE is about 31% of the encryption using divergent illumination and asymmetric keys which shows that the result are good in comparison of the encryption using divergent illumination and asymmetric keys.

***Keywords*—** Optical Image Encryption, Secure Hash Algorithms, Keyless Encryption.

## I. INTRODUCTION

With the worldwide use of internet and networking, millions of transactions are performed everyday ranging from exchange of credit card data to using an identity proof for identification. Ensuring the safety of data being exchanged is significant. With a rising amount of sensitive and mission critical-data in flight around the clock, the mainstream of organizations are actively working to develop offensive strategies against the inexporable and constantly evolving threatscopes. Every year millions of dollars are spent on deterrence of data frauds, including credit card forgery. Although the people are not aware of it, scientists are developing different image encryption techniques in order to protect important data specifically in data transmission. Presently some encryption algorithms are proposed to secure electronic communication, such as AES (Advanced Encryption Standard), which is a symmetric key algorithms means that the encryption and decryption keys are same. Moreover there is a Rivest-Shamir-Adleman (RSA) algorithm which is an asymmetric algorithm means there is a public key for encryption and an associated private key for decryption. But the problem with encryption using keys is that they are vulnerable to different types of attacks and lead to compromise the security of the system. To improve the security, a new image encryption technique that uses a keyless approach for image encryption is proposed. Keyless approach increases the ability of the system from different types of attacks as compared to the asymmetric keys that are vulnerable to various types of attacks. For security check of the system hash algorithms (MD5 and SHA128) are applied which checks whether the image transmitted over the web is manipulated in between the transfer from sender to the receiver. The image is encrypted in such a way that it is not an easy task for the third party to recognize or create the original image by just seeing the encrypted image. Before the transfer of the image SHA128 and MD5 of the image is calculated. After the decryption of the image if SHA128 and MD5 of the system matches the image is not manipulated otherwise it is manipulated. So the Keyless approach, SHA128 and MD5 together increases the overall security of the system and make the system more secure by protecting it from different types of attacks.

## II. RELATED WORK

In the year 1994 Philippe Refregier, BahramJavidi[8] the first image encryption *technique DRPE (Double Random Phase Encryption)* started. In DRPE, the image is encoded with the help of two random phase masks and classical 4-f correlator into the noise like image. In the previous time it is combined

with the Fresnel transform, the fractional fourier transform, gyrator transform and phase truncation operations. To advance the security of DRPE, it is now been combined with other optical imaging techniques such as photon-counting imaging, iterative computational algorithms and compressive sensing. DRPE is one of the most popular optical image encryption method due to its straight forwardness.

*DRPE with Photon Counting*: A photon-counting (PC) technique[13] has been combined with the DRPE technique for encryption and security verification. By combining DRPE with Photon counting it present an additional security layer against attacks. In photon counting imaging, the number of photons that arrive at a pixel can be restricted through a stochastic Poisson process. A sparse encrypted image is obtained by limiting the number of photons. As a result, the resultant decrypted image does not disclose the original information.

*Optical Encryption based on Diffractive Imaging***:** An optical multiple random phase mask encoding system is applied and one of the phase-only masks is chosen and laterally translated along a preset direction throughout the encryption process.[7] For image decryption, a phase retrieval algorithm is used to extract a high quality plaintext. The feasibility and effectiveness of the method are demonstrated by numerical results. This method can provide a new strategy as a substitute of conventional interference methods.

In the above strategy all process is done on the symmetric keys.

*Asymmetric key Encryption*

*Asymmetric Cryptosystem based on Phase Truncation Fourier Transform:* [26] With the phase truncation in Fourier transform, one can be capable to produce an asymmetric ciphertext as real-valued and stationary white noise by using two random phase keys as public keys, while a authorized user can retrieve the plaintext using another two different private phase keys in the decryption process. The nonlinear operation of phase truncation, high robustness against existing attacks could be attained.

*Asymmetric Cryptosystem based on EMD***:** [27] The equal modulus decomposition (EMD) is an asymmetric cryptosystem based on coherent superposition which can oppose the specific attack. In this paper, we counter the vulnerability through an encoding technique which uses multiple diffraction intensity pattern recordings as the input to the EMD set up in the gyrator domain. This allows suppression of the random phase mask in the EMD path. As a result, the scheme achieves resistance to specific attack. The simulation results and the security analysis reveals that EMD based on multiple intensity pattern recording is an effective optical asymmetric cryptosystem suitable for securing data and images.

*OPTICAL IMAGE ENCRYPTION BASED ON INTERFERENCE* **:** [28] A novel architecture for optical image encryption based on interference. The encryption algorithm for this new method is quite simple and does not need iterative encoding. The parameters of the configuration can also serve as supplementary keys for encryption. Numerical simulation results display the flexibility of this new method.

*Optical Image Encryption Using Divergent illumination and asymmetric keys:* [1] In this scheme, the input image is encrypted by use of two random phase masks (RPMs) located at the input and the conjugate plane in a diverging spherical wavefield. Contrast with the schemes using planar illumination and symmetric keys, a significant variation is that constant change of positions of optical elements applied for encryption is allowed, resulting in decryption keys that are different from the encryption keys(or their conjugates) and inconsistent size display of encrypted/decrypted images.

## III. METHODOLOGY

The algorithm of the proposed work is as follows:

**Setup**

Initialize all required variables

**Encryption**

Step1. I← read an image

Calculate MD5 and SHA128 of the original image

Step2. R← get red channel of the image

Step3. G← get green channel of the image

Step4. B← get blue channel of the image

Step5. Loop till end of the image pixel

← R (i, j, k) + L value

[b b1]← perform discrete wavelet transformation on the pixel using db1

← replace matrix value with b

End loop

Step6. Repeat step 5 for green and blue channel

Step7. newImage←[R, G, B]// create new image

**Decryption**

Reverse steps to get decrypted value

Step1. Get R, G, B channels from the new image

Step2. Get inverse of DWT

Step3. Subtract L value

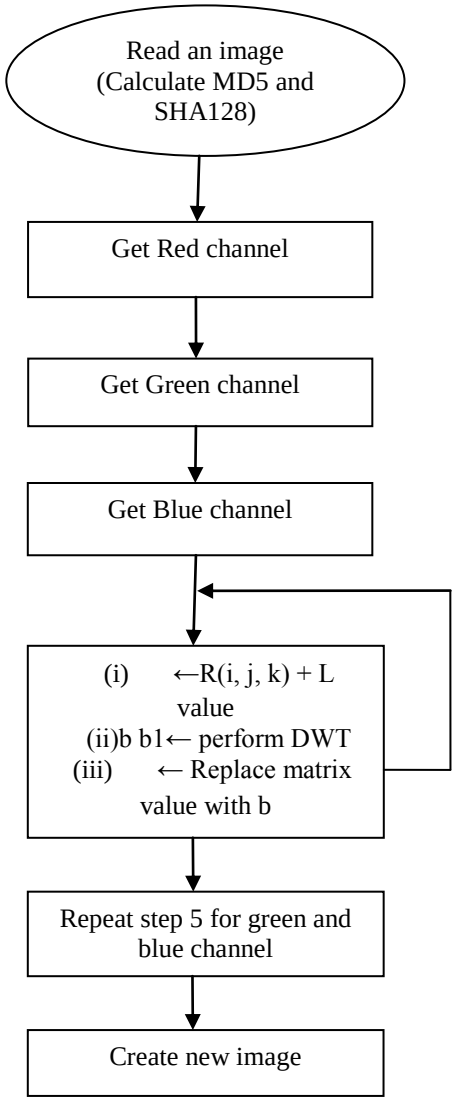
Step4. Put R, G, B in one matrix to get the decrypted image.

**Testing**

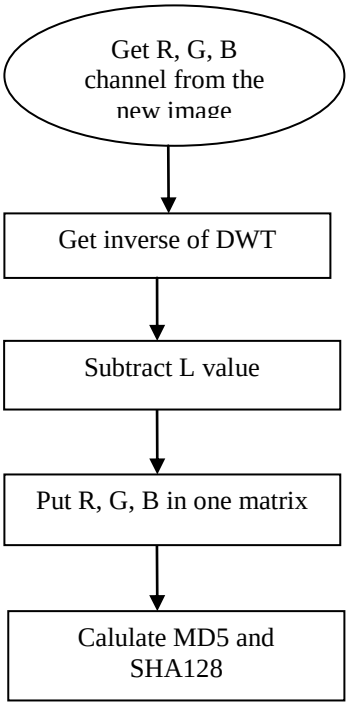
Perform MSE, PSNR on the original and decrypted images. Calculate MD5 and SHA128 of the decrypted image, compare with original values.

The flowcharts of the proposed scheme are:

**Encryption Scheme:**




**Decryption Scheme:**




## IV. RESULTS AND DISCUSSION

Let a = 1 2 3 4
4 5 6 8
2 7 6 3
5 9 8 2

be the matrix of dimension 4x4.

To get L value, we have to add any random value to a (i.e 128)

L value= a+128

L value= 129 130 131 132
132 133 134 136
130 135 134 131
133 137 136 130

By applying discrete wavelet transform on first value of the matrix we get,

dwt ((1+128),'db1')

ans =182.4335

same for the other values i.e.

dwt ((4+128),'db1')

ans =186.6762

dwt ((2+128),'db1')

ans = 183.8478

By applying discrete wavelet transform:

[b b1]= dwt (50,'db1')

b = 70.7107

b1 = 0

From the arrangement of encryption and decryption scheme, we can see that the original and the encrypted image are different from each other and no one recognize the original image by seeing the encrypted image. By seeing the encrypted image even the user cannot recognize the original image so it is very difficult task for the third party to create the original image by just seeing the encrypted image. So the data sent over the web is secure and even if someone is able to see it, he/she will not get the idea what is it.

Diagrammatic representation of the scheme:

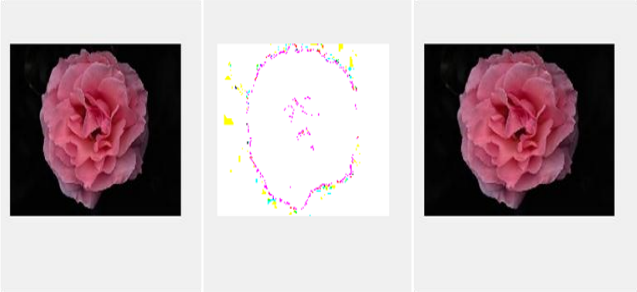


Fig.1(a)Original image(b) Encrypted image(c) Decrypted Image.

COMPARISON OF VALUES OF MSE OF BOTH SCHEMES

| S.No. | Encryption using Divergent illumination and asymmetric keys | Proposed | D= (Base-Proposed) | P=D/Base*100 | Result =(100-P) | Image Code |
|---|---|---|---|---|---|---|
| 1 | 0.00119087 | 0.000296406 | 0.000894464 | 75.110 | 24.890 | 202 |
| 2 | 0.00128345 | 0.000319551 | 0.000963899 | 75.102 | 24.898 | 201 |
| 3 | 0.00195733 | 0.00048802 | 0.00146931 | 75.067 | 24.933 | 202 |
| 4 | 0.00149222 | 0.000371744 | 0.001120476 | 75.088 | 24.912 | 203 |
| 5 | 0.00145824 | 0.000363248 | 0.001094992 | 7.508 | 92.492 | 312 |
| 6 | 0.00105412 | 0.00026222 | 0.0007919 | 75.124 | 24.876 | 300 |
| 7 | 0.00124292 | 0.000309419 | 0.000933501 | 75.106 | 24.894 | 302 |
| 8 | 0.00144482 | 0.000359919 | 0.001084901 | 75.089 | 24.911 | 305 |
| 9 | 0.00157242 | 0.000391795 | 0.001180625 | 75.083 | 24.917 | 308 |
| 10 | 0.00148171 | 0.000369116 | 0.001112594 | 75.089 | 24.911 | 310 |

Table No.1. Values of MSE for both the schemes

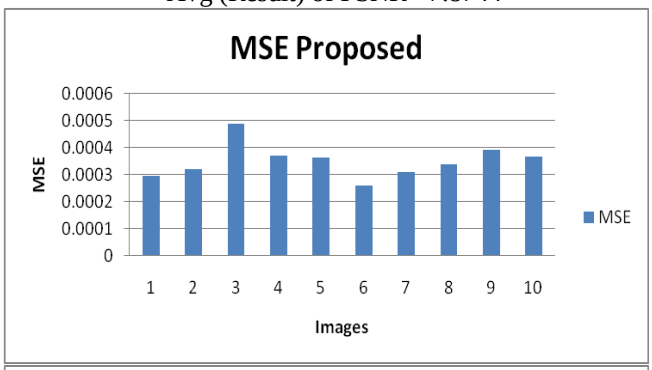
Avg (Result) of MSE = 31.6634

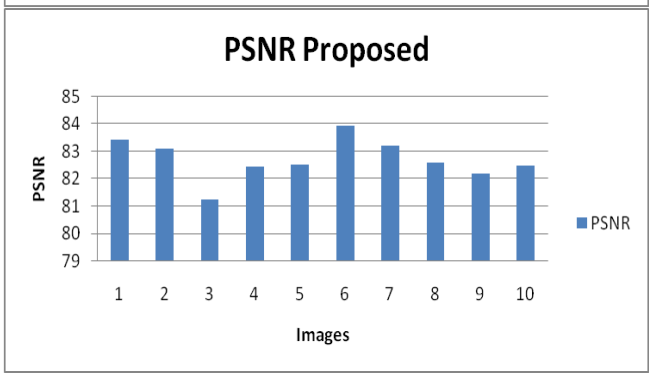
COMPARISON OF VALUES OF PSNR OF BOTH SCHEMES:

| S.No | Encryption using Divergent illumination and asymmetric keys | Proposed | D= (Proposed-Base) | Result= D/Base * 100 | Image Code |
|---|---|---|---|---|---|
| 1 | 77.3722 | 83.4119 | 6.0397 | 7.806 | 200 |
| 2 | 77.047 | 83.0854 | 6.0384 | 7.837 | 201 |
| 3 | 75.2142 | 81.2464 | 6.0322 | 8.020 | 202 |
| 4 | 76.3925 | 82.4284 | 6.0359 | 7.901 | 203 |
| 5 | 76.4925 | 82.5288 | 6.0363 | 7.891 | 312 |
| 6 | 77.9019 | 83.9941 | 6.0422 | 7.756 | 300 |
| 7 | 77.1864 | 83.2253 | 6.0389 | 7.824 | 302 |
| 8 | 76.5324 | 82.5688 | 6.0364 | 7.887 | 305 |
| 9 | 76.1651 | 82.2002 | 6.0351 | 7.924 | 308 |
| 10 | 76.4232 | 82.4592 | 6.036 | 7.898 | 310 |

Table No.2. Values of PSNR for both the schemes

Avg (Result) of PSNR= 7.8744




Two Error metrics are used to compare the various image encryption techniques are the: Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR).

The MSE is the cumulative squared error between the encrypted and the original image.

PSNR is a evaluation of the peak error.

PSNR= 20*log10 (255/sqrt (MSE)

A low value of MSE means less error and there is an contrary relation between the MSE and PSNR, this translates to a higher value of PSNR. Logically, a elevated value of

PSNR is good because it means that the ratio of Signal to Noise is higher. Here, the signal is the original image and the noise is the error in reconstruction of the image. So, if you find a compression scheme having a lower MSE (and higher PSNR), you can find that it is a better one.

The results shows that the value of error matrix, PSNR is increased by approximately 8% and the values of MSE is about 31% of the base scheme which shows that the result are good as compared to the base scheme. So the proposed scheme is more effective in optical image encryption and can be applied for image encryption in different fields which requires the high level of security.

## V. CONCLUSION AND FUTURE SCOPE

The paper presented an idea of making more efficient and reliable image encryption scheme. In this paper a keyless approach for image encryption is presented that allow the system to encrypt the image by the use keyless image encryption scheme. The proposed approach aims to complete the task of image encryption without the manipulation of the image at receiver side, for that hash functions are applied. This feature makes the system more secure and reliable. Any user can calculate the value of hash functions (SHA128 and MD5) before the transfer of the image and check it after the decryption of the image. If the value of SHA128 and MD5 matches the image is not manipulated. This feature makes it more secure as compared to the other techniques. The results shows that the value of error matrix, PSNR is increased by approximately 8% and the values of MSE is about 31% of the base scheme which shows that the result are good as compared to the base scheme. So the proposed scheme is more effective in optical image encryption and can be applied for image encryption in different fields which requires the high level of security. It is also observed that the encrypted image is completely unrecognizable from the original image so it is a tough task for the third party to guess the original image and the risk of data fraud is decreased in the proposed scheme.

## *REFERENCES*


[1] Xiaogang Wang, Guoquan Zhou, Chaoqing Dai, Junlang Chen "Optical Image Encryption Using Divergent illumination and asymmetric keys", IEEE Photonics Journal Volume 9, Number 2, April 2017.

[2] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki "A Novel Image Encryption Algorithm Based on Hash Function" IEEE 2010.

[3] M.Dileep, B.Prudhviraj, G.Prasannakumar" A New Image Encryption and Data Hiding Technique Using Wavelet Transform",IJRET, Volume: 05 ,05- May-2016.

[4] R.Sivamalar, Dr.Swati Sharma "Survey on Various Optical Image Encryption Techniques" *ETEBMS* - November 2016.

[5] M.A. Mohamed**,** A.S. Samarah, M.I. Fath Allah **"** Optical Encryption Techniques: An Overview" IJCS, Vol. 11, Issue 4, 2 July 2014.

[6] ShiLiu, Changliang Guo, JohnT.Sheridan" A review of optical image encryption technique"Elsevier 2013.

[7] WenChen,, XudongChen, ColinJ.R.Sheppar "Optical image encryption based on diffractive imaging" Optics Lett. Vol.35,No.22 November15,2010.

[8] Philippe Refregier, BahramJavidi" Optical image encryption based on input plane and Fourier plane random encoding" Optics Lett.,Vol.20,No.7, April1,1995.

[9] Jun Li, Jiao Sheng Li, Yang Yang Pan, Rong Li "Compressive Optical Image Encryption" *Scientific Reports* **5**, Article number: 10374 (2015).

[10] Palwinder Singh**"** Wavelet Transform in Image Processing: Denoising, Segmentation and Compression of Digital Images**"** IJSRSET ,Volume 2, Issue 2, 2016

[11] Jun-Xin Chen, Zhi-Liang Zhu, Chong Fu, Li-Bo Zhang, Yushu Zhang "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding" journal of optics, Volume 16, October 15,2014.

[12] Xiang Peng, Peng Zhang, Hengzheng Wei, and Bin Yu "Known-plaintext attack on optical encryption based on double random phase keys", optics Lett, volume 31,2006.

[13] Elisabet Pérez-Cabré, Myungjin Cho, and Bahram Javidi " Information authentication using photon-counting double-random-phase encrypted images", optics Lett, volume 36,2011.

[14] Guohai Situ and Jingjuan Zhang "Double random-phase encoding in the Fresnel domain", optics Lett, volume 29,2004.

[15] Wen Chen, Bahram Javidi, and Xudong Chen " Advances in optical security systems", Advances in Optics and Photonics,Volume 6,2014.

[16] Shi Liu, John T. Sheridan," Optical encryption by combining image scrambling techniques in fractional Fourier domains" Elsevier, volume 287, 15 January 2013

[17] Shi Liu, Bryan M. Hennelly, John T. Sheridan" Numerical simulation of double random phase encoding",2012.

[18] Surbhi Aggarwal, Neha Goyal, Kirti Aggarwal "A review of Comparative Study of MD5 and SHA Security Algorithm", IJCA,Volume 104,October14, 2014.

[19] Arturo Carnicer, Mario Montes-Usategui, Sergio Arcos, and Ignacio Juvells "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys" , Optics Lett,Volume 30, 2005.

[20] Yann Frauel, Albertina Castro, Thomas J. Naughton, and Bahram Javidi "Resistance of the double random phase encryption against various attacks", Optics Express, Volume 15, 2007.

[21] P.M. Bentley, J.T.E. McDonnell "Wavelet transforms: an introduction" Volume: 6, Aug 1994.

[22] Sandhya Verma,G.S. Prajapati "Robustness and Security Enhancement of SHA with Modified Message Digest and Larger Bit Difference", IEEE,September 19,2016.

[23] K. Saravanan 1,A. Senthilkumar "Theoretical Survey on Secure Hash Functions and issues" IJERT, Vol. 2 Issue 10, October – 2013.

[24] Bahram Javidi and Jun Wang "Design of filters to detect a noisy target in non overlapping background noise", Volume 11, 1994.

[25] Bahram Javidi, Farokh Parchekani, and Guanshen Zhang "Minimum-mean-square-error filters for detecting a noisy target in background noise", volume 35,1996.

[26] Wan Qin and Xiang Peng "Asymmetric cryptosystem based on phase-truncated Fourier transforms",Optics Letters , Vol. 35,2010.

[27] Jianjun Cai, Xueju Shen, Ming Lei, Chao Lin, and Shuaifeng Dou, "Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition", Optics Letters ,Vol. 40,2015.

Yan Zhang and Bo Wang "Optical image encryption based on interference",Optics Letters ,Vol. 33,2008.