International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

REVIEWONVARIOUSIMAGEENCRYPTIONMETHODS

RENU BUNDEL SHAKYAWAR, ABINASH KUMAR
PG Scholar, ECD, Dr. APJ Abdul Kalam University Indore, M.P., India
Assistant Professor, ECD, Dr. APJ Abdul Kalam University Indore, M.P., India

ABSTRACT: Image encryption has been a popular research field in recent decades. This paper reviews various image encryption schemes, in terms of better performance in terms of randomnessproperties and security level. Image encryption needs to provide the necessary properties for a secureimage encryption scheme including confusion and diffusion properties. Image encryption schemesmust satisfy the required performance tests such as large key space, high high-severity and acceptableencryption speed. These characteristics make it a suitable candidate for use in cryptographic applications. Literature survey aims to explore all the past analysis works performed within the concernedresearchtopic; so that new concepts will be generated for future work. The literature survey has seen anyanalys is works performed for encoding and cryptography of a picture

Keywords:*Cryptography;ColorImage;Algorithm ImageEncryption,Image encryption, Artificial intelligence*

INTRODUCTION

With the ever-expanding development of sight and sound applications, security is an imperativeissue in correspondence and the capacity of pictures, and encryption is of one the approaches to guarantee security. Picture encryption has applications in the web, mixed media frameworks, correspondence, telemedicine, clinical imaging, and military correspondence. Presently an ever-increasing number of investigations have been created for security issues to shield theinformation from conceivable unapproved guidelines. There as of now exist a few pictureencryption strategies. Notwithstanding, every one of them has its quality and shortcomingsregarding security level, speed, and coming about stream size measurements. We

consequentlyproposed a new encryption technique to beat these issues. The proposed picture encryptiontechniquedepends on revamping the picture's pixels. Theadjustmentisfinishedbycheckingdesignscreatedbytheſ SCANapproach.Thecheckingwayofthe pictureisanarbitrarycodestructure,andbydeterminingthepixelsarrangementalongthefilteringway. Notethatcheckingwayofapictureisessentiallyarequestinwhicheverypixelofthepictureisgottentopr eciselyonce.Suchtheencryptionadditionallyincludesthedeterminationofsetmysterycheckingways .Consequently,theencryptionneedsasystemto determine and produce a bigger number of wide assortments of checking ways successfully.Thesecurityofcomputerizedpicturesincludesafewuniqueviewpoints,includingcopyri ghtinsurance,validation, classification, and access control

LITERATUREREVIEW

The purpose of literature survey is to explore all the past research works performed in theconcerned research topic; so that new ideas can be generated for future work. The literature surveyhave gone through several research work performed for Encryption and Decryption of an image.Thesurveyis as followed:-

Liu et al [2011] presented an Image encryption algorithm base on chaos theory. This paperintroducesamethodofimageencryptionalgorithmchaoticsequence.Chaoticsequenceisg enerated by the Logistic mapping .In this method image encryption is realized by the gray value ofsubstitutes and pixel position scrambling.The Encryption algorithm has the big key space, it isalso difficult to decipher It has relatively good properties in anti-damaged and correlation inaspectsof statistical attacks[1].

Panicker et al [2010] presented an Image Encryption and Decryption Using Sandwich PhaseDiffuser and False Image along with Cryptographical Enhancement. The encryption is done byemploying a sandwich phase diffuser made by using two speckle patterns, and

placed in theFourier plane of a double random phase encoding system. After phase diffusion another image isfused to the resultant image and then cryptographical enhancement is done which provide anadditional security to the system. The used cryptographic technique is derived from the AEScryptosystem in which a modified shift row operation is performed. During decryption firstinverse cryptographical enhancement is done, followed by subtraction of the fused image. Thenfurther decryption process will be done. The reliability of the technique is evaluated using MeanSquareError (MSE)calculation between thedecryptedand original image[2].

Anane et al [2010] presented a RSA Based Encryption Decryption of Medical Images. In thispaper medical images are encrypted and decrypted by the RSA cryptosystem (public key encryption)and tested on medical images. The encryption and decryption of medical images are performedby software. A software implementation has the advantage of being portable and low-cost.However, software implementation of RSA protocol remains slow because medical images largeandthe sizes of thekeysarein therangeof(1024-2048)bits [3].

Pandurangaetal[2010]presentedaHybridapproachforImageEncryptionUsingSCANPatternsandCarrierImages.Thereisahybridtechniqueforimageencryptionthatemploysthe concept of carrier image and SCAN patterns generated by SCAN methodology. Although itinvolves existing methods like SCAN methodology, the novelty of the work lies in hybridizingand carrier image creation for encryption. Here the carrier image is created with the help ofan alphanumerickeyword.Eachalphanumerickeywillhaveaunique8-bitvaluegeneratedby4 out of 8 codes. This newly generated carrier image is added tothe original image to obtainthe encrypted image. The scan methodology is applied to either the original image or carrier image, afterthe addition of the original image and carrier image to obtain the highly distorted encrypted image. Theresulting image is found to be more distortedin the hybridtechnique. By applying the reverseprocessweget thedecrypted image [4].

Parameshachari etal [2010] presented a secure partial image encryptionscheme using scanbased algorithm. The focus of this paper is on selecting the important part of the image that canbe efficientlyachievedbyconceptuallyselectingtheimportantpartoftheimage.Thispaperpropose s a new approach for partial image encryption using the SCAN algorithm. The main ideabehindthepresentworkistoselectthepartoftheimageperformedbySCAN-basedpermutation of pixels and substitution rule which together form an iterated product cipher. Theissue in traditional cryptosystems in many different areas such as wireless networking, mobilephone services, and applications in homeland security isenergy consumption for encryption ofthelargevolumeof visual data. So wearedealingwithpartial encryption[5].

Jinping et al [2009] presented a Color image encryption and decryption based on a double randomphase encoding technique. The color image to be encrypted is first separated into three colorchannels: red (R), green (G) and blue (B). Each of these channels is encrypted using a doublerandom phase encodingtechnique andthen threenewcoding image matrixes are constructed.We choose a large enough absolute symmetric image as the host image which has also been segregatedinto tricolor channels to hide the real and imaginary parts of the encoding data and discuss themethod how constructing the complete symmetrical host image. On the receipted side simpleextracted and decryptionoperations can be employed to obtain thereconstructed image that isthesame as the original image[6].

Chen et al [2008] presented a Multiple-Image Encryption by Rotating Random Grids. In thispaper visual secretsharing (VSS) technique encryptsa secretimage into severalsharedimages and, later, decrypts the secret by stacking the shared images and

recognizing them by the humanvisual system. The main advantages of VSS by adopting randomgrids comparedwith VCinclude no pixel expansion and no cost of sophisticated codebook design. In this paper, theauthors present the new scheme which encrypts two secret images into two random grids withoutany pixelexpansionand,later, decryptstheoriginalsecretsby directly stacking tworandomgridsin anadditionalwayofrotatingonerandomgrid at 90,180 or 270degrees[7].

Sheshadrinathan et al [2008] presented an Advanced Encryption Standard for the Encryption andDecryption of Images and Text on a GPU. In this paper, the author proposes a system for thecompleteimplementationoftheAdvancedEncryptionStandard(AES)forencryptionandde cryption of images and text on a Graphics Processing Unit. The GPU acts as a valuableCoprocessor that relieves the load off the CPU. In the decryption stage, we use a novel techniqueto displaythedecrypted images and text on the screen without bringingit onto CPUmemory[8].

Sawada et al [2006] presented an Image Encryption and Decryption using an Optical PhaseMask. In this paper, a novel encryption method as an optical architecture of cryptography, basedon the grouping of the information in the Fourier plane. This grouping is termed segmentation; itwas been used to make the so-called segmented filter used in optical target recognition tooptimize the performances of the correlator decision. By using the concept of segmented filter,encryption can be considered as an image encrypting with a segmented phase mask called keysand consists of modifying the phase profile of the original image by multiplying it by the adaptedphase mask.Inour case,thiskey willgroupinformationgatheredfromdifferentsub-keysaccordingtoawell-definedcriterion.Thedecryptionissimplyperformedbyanopticalcorrelation by using a composed correlation filter, since the encryption keys are complex images,theycannot be randomlyfoundin a reasonable time[9].

Chen et al [2006] presented an Image encryption and decryption using SCAN

methodology. Thispaper shows the way to encrypt and decrypt the image by using the SCAN algorithm. In this methodgrayimageisencryptedbyspatialaccessingthat isscanning.Thisproducestheencryptionkeys

in very many ways. This encryption method is based on the rearrangement of pixels. The pixelarrangementis dependent on the encryption key[10].

Mniccam et al [1999] presented a Scan Based Lossless Image Compression and Encryption. Thispaper presents a new methodology that performs both lossless compression and encryption ofbinary and gray-scale images. The compression and encryption schemes are basedon ScanpatternsgeneratedbytheScanmethodology.Thedrawbackofthemethodologyisthatcompression -encryptiontakes a longer time[11].

CONCLUSION

Thisprogressiveageofmixedmediaandorganizationsisutilizinganever-increasingnumberofpicturesandtransmissionamongthePCframeworks.Thepicturesecurityis of considerable imperativeness nowadays. In this postulation, the answers for guaranteeingthe security of the picture have been improvised. The sweep put-together encryption strategy is basedonthe improvement of the pixel. The pixel plan relies upon unscrambling the key. Ifthe past strategy is thought about, the security is improved which has appeared in theoutcome.securityisaccumulatedbycheckingthe entirepictureafterexaminingeachsection.Accordingly,theresultantscrambledpictureseems,byall accounts, to be a single picture and the cycle of encryption is practically erratic. The proposedencryption strategy can accomplish two objectives. One is to configure profoundly and make sureabout the picture cryptosystem. The other is to decrease the ideal opportunity for encryption anddecoding. There are numerous highlights of the sweep strategy, for example, Lossless encryptionof picture, expanded Security by the utilization of more than a few encryption circles, Improbablechanceofencryptionkeyguessing,effectivelyimplementableinequipment,andSeveralap

plications in web correspondence, interactive media framework, clinical imaging, telemedicine,andmilitarycorrespondenceand soforth.

REFERENCES

1. Omar Reyad Omar Reyad; M. A. Mofaddel; W. M. Abd-Elhafiez; Mohamed Fathy *A NovelImageEncryptionSchemeBasedonDifferentBlockSizesforGrayscaleandColorImages*10.1109/ICCES.2017.8275351ComputerEngineeringandSystems(ICCES),201712thInternationalConferenceCairo, Egypt
2. ChunhuLi,GuangchunLuo,andChunbaoLi,*An Image EncryptionSchemeBasedonTheThree - dimensional Chaotic Logistic Map,* International Journal of Network Security, Vol.21, No.1,PP.22-29,Jan. 2019 (DOI: 10.6633/IJNS.20190121(1).04) 22
3S.SowmiyaI.MonicaTresaA.PrabhuChakkaravarthy*PixelBasedImageEncryptionUsingMagic Square*ie2016
4. Joshua Caleb Dagadu; Jian-Ping Li; Fadia Shah; Nadir Mustafa; Kamlesh Kumar DWT-basedencryption technique for medical images 13th International Computer Conference on WaveletActiveMedia TechnologyandInformation Processing(ICCWAMTIP)Year: 2016
5. A new chaos-based image cipher using a hash function Fu; OuBian; Hui-yan Jiang; Li-huiGe;Hong-FengMar2016IEEE/ACIS15thInternationalConferenceonComputerandInformationScience(ICIS)
6. D.I.GeorgeAmalarethinam,J.Geetha,‖EnhancingSecurityLevelforPublicKeyCryptosystem Using MRGA‖, World Congress on Computing and Communication Technologies(WCCCT),2014Pages 98-102.ISBN:978-1-4799-2876-7.
7. A Novel Cryptographic Encryption Technique for Securing Digital Images the Cloud UsingAES and RGB Pixel Displacement Quist-Aphetsi Kester;Laurent Nana; Anca Christine Pascu2013European ModellingSymposium
8. Z. Liu, L. Xu, C. Lin, J. Dai, and S. Liu, ―Image encryption scheme by using iterative randomphase encoding in gyrator transform domains,‖ Optics and Lasers in Engineering, vol. 49, no. 4, pp.542–546, 2011.
9. G. Zhang and Q. Liu, ―A novel image encryption method based on total shuffling scheme,‖Optics Communications,vol. 284, no. 12, pp. 2775–2780, 2011.
10. Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, ―A chaos-based symmetric image encryptionschemeusingabit-levelpermutation,‖ InformationSciences,vol. 181,no.6,pp.1171–1186,2011.
11. Y. Wang, K. W. Wong, X. Liao, and G. Chen, ―A new chaos-based fast image encryptionalgorithm,‖Applied SoftComputingJournal, vol.11,no. 1, pp. 514–522, 2011.
12. X. Y. Wang, L. Yang, R. Liu, and A. Kadir, ―A chaotic image encryption algorithm based onperceptronmodel,‖ Nonlinear Dynamics,vol.62, no. 3, pp. 615–621,2010.
13. Q. Guo, Z. Liu, and S. Liu, ―Color image encryption by using Arnold and discrete

fractionalrandom transforms in IHS space,‖ Optics, and Lasers in Engineering, vol. 48, no. 12, pp. 1174–1181, 2010.

14. R. Tao, X. Y. Meng, and Y. Wang, ―Image encryption with multi orders of fractional Fouriertransforms,‖ IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 734–738,2010.
15. Z. Lin and H. Wang, ―Efficient image encryption using a chaos-based PWL memristor,‖ IETETechnicalReview, vol. 27, no. 4, pp. 318–325, 2010.
16. Gopinath Ganapathy, and K.Mani, ― Add-On Security Model for public key CryptosystemBased on Magic Square Implementation‖, ISBN 978-988- 17012-6-8, Proceedings of the World Congresson Engineeringand Computer Science2009 VolI,SanFransisco,US
17. C.K.HuangandH.H.Nien,―Multichaoticsystemsbasedpixelshuffleforimageencryption,‖ OpticsCommunications, vol. 282, no. 11, pp. 2123–2127, 2009.
18. MohammadAliBaniYounesandAmanJantan,―Image EncryptionUsingBlock-BasedTransformationAlgorithm‖,IAENGInternationalJournalofComputerScience,35:1,IJCS_35_1_03,19 February2008.
19. A. Gutub, M. Ankeer, M. Abu-Ghalioun, A. Shaheen, and A. Alvi, ―Pixel indicator highcapacity technique for RGB Applications(WoSPA 2008)University of Sharjah, Sharjah, U.A.E.,2008
20. M.T.Parvez and A.A.A. Gutub, ―RGB intensity based variable bits Image Steganography‖ intheproceedings of AsiaPacific ServicesComputingConference(2008)
21. S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. T. Lo, ―A general quantitative cryptanalysis ofpermutation-onlymultimediaciphersagainstplaintextattacks,‖SignalProcessing:ImageCommunication,vol. 23,no. 3, pp. 212–223, 2008.
22. C. K. Huang, H. H. Nien, S. K. Changchien, and H. W. Shieh, ―Image encryption with chaoticrandom codes by grey relational grade and Taguchi method,‖ Optics Communications, vol. 280, no.2, pp.300–310, 2007.
23. T.Xiang,X.Liao,G.Tang,Y.Chen,andK.W.Wong,―Anovelblockcryptosystembasedonite ratingachaoticmap,‖PhysicsLetters,Section A,vol. 349,no. 1–4, pp.109–115, 2006.
24. K. W. Wong, S. W. Ho, and C. K. Yung, ―A chaotic cryptography scheme for generating shortciphertext,‖PhysicsLetters, SectionA,vol. 310, no.1, pp. 67–73, 2003.
25. X.-Y. Zhao and G. Chen, ―Ergodic matrix in image encryption,‖ in Proceedings of the 2ndInternationalConferenceonImageandGraphics,vol.4875, pp.394–401, August2002
26. R. Zunino, ―Fractal circuit layout for spatial decorrelation of images,‖ Electronics Letters, vol.34, no. 20, pp. 1929–1930, 1998.
27. Z. Liu, H. Chen, T. Liu, et al., ―Image encryption by using gyrator transform and Arnoldtransform,‖Journal of ElectronicImaging,vol. 2,no. 4, pp.345–351, 1993.
28. G. Chen, Y. Mao, and C. K. Chui, ―A symmetric image encryption scheme based on

3Dchaoticcatmaps,‖Chaos,SolitonsandFractals,vol.21,no.3,pp.749–761,2004.ViewatPublisher·View at Google Scholar·View at Scopus

29. S. Mazloom and A. M. Eftekhari-Moghadam, ―Color image encryption based on CoupledNonlinearChaoticMap,‖Chaos,Solitons andFractals, vol.42, no.3, pp.1745–1754, 2009.

30. Y. Tang, Z. Wang, and J. A. Fang, ―Image encryption using chaotic coupled map lattices withtime-varyingdelays,‖CommunicationsinNonlinearScienceandNumericalSimulation,vol.15,no.9,pp.2456–2468,2010.O.Edward,ChaosinDynamicalSystems,CambridgeUniversityPress,Cambridge, UK, 2nd edition, 2003.

M. S. Baptista, ―Cryptography with Chaos,‖ Physics Letters, Section A, vol. 240, no. 1-2, pp.50–54, 1998.