A Hybrid Image Encryption Using Digital Image Fusion With Standard Encryption

Rajeshkumar S[1], Manjupreethi B[2], Narmadha Shri N[3], Ponselvi S[4]

[1] *Assistant Professor, Department of Electronics and Communication Engineering, V.S.BEngineeringCollege, Karur, Tamilnadu, India,* *rajesh9225006@gmail.com*
[2,3,4] *U.G.Student, Department of Electronics and Communication Engineering, V.S.BEngineeringCollege, Karur, Tamilnadu, India,* *manjupreethi.b@gamil.com, narmadhashri77@gmail.com, ponselvi2301@gmail.com*

Abstract-Rows-columns diffusion, the 3Dscale-invariantmodularchaoticmap, and Hilldiffusion are the three key phases in this study. Using rows-columns diffusion and Hill diffusion, pixels are substituted and the plain image's adjacency pixels are combined. 3Dscale-invariantchaoticmaps are used to overmute picture pixels without restricting the image size. When at least two rounds of significant stages are repeated, the suggested encryption system approaches. It's also particularly sensitive to little differences in the plainimage and the secretkey. As a consequence, selected/known plaintextassaults are successfully thwarted. Experiments have shown that the suggested approach works..

IndexTerms–*Chaotic map, hill diffusion,encryption*.

I.INTRODUCTION

Advances in information technology (IT), especially in communication and social networks, have made it feasible to offer digital multimedia material to a huge number of individuals in the online world. However, a rising variety of digital materials, such as image, video, and audio processing environments, as well as Internet access through personal computers, are now accessible globally. Smartphones have established a perfect way for distributing and sharing multimedia material that is overly overwhelming. The most important. For this, the present task is to safeguard intellectualpropertysecurityriskstomultimediacontentontheinternet. As a result, security is becoming more important in today's public Internet gateway of information.

Information and multimedia security is the activity of preventing unauthorised access, use, disclosure, interruption, alteration, inspection, recording, or destruction of information[4].

The three most critical aspects of information security are confidentiality, integrity, and availability. To accomplish these aims, security mechanisms like as encryption, authentication, and authorisation, to mention a few, are utilised. Symmetric publickey (asymmetric) cryptography and shared key cryptography are the two most common forms of encryption methods. In the case of data or information, symmetric or sharedkeyencryption techniques are reliably utilised. In most cases, publickeyencryption is used to offer security. Integrity, non-repudiation, and authenticity services employing digital signatures Multimodaldata confidentiality, including picturesecrecykeyencryption approaches, are used due of the speed of cryptography.

II. RELATEDWORK

One of the key concerns of users is the security and safety of data and multimedia, such as photographs, throughout processing, storage, and transmission. Digitalimagecryptographyis one of the most well-known strategies for maintaining image secrecy and integrity across an unsecured public channel like the internet [16]. Due to the vulnerability of public Internet routes to assaults, effective cryptography methods are required for safe data and multimedia transfer[13]. From the perspective of an image cryptanalyst, ProfessorChengqingLiandetal. examined papers and research on picture encryption techniques and algorithms offered in 2018. Various digital picture encryptions that have been suggested in the literature will be evaluated in this section.

2.1.Standardcryptography

Strictly speaking, there are three types of encryption methods: symmetricblockcipher, symmetricstreamcipher, and asymmetric cypher.

DES and AES are the most widely used symmetric block cyphers for encrypting data and pictures.

An image encryption software based on AES in cypher block chaining (CBC) mode was built using Clanguage by YongZhang inref[5].

V.M.Silva-Garca et al.expand the block cypher tripleDES(3DES) to a 96-bit encryption dubbed Triple-DES-96, which is used to encrypt colour images.

ManjuKumarietal has examined and developed the majority of encryption techniques and algorithms based on symmetric block cypher (DES, AES, 3DES) and symmetric stream cypher (RC4,RC6). [9]. Because asymmetric encryption techniques like RSA and ECC are slow, picture encryption is employed seldom. Theintegrityandauthenticationwiththehelpofwatermarkingandsteganographytechniquesandsoonarethemostcommonusesofthis typeofencryption.

2.2.Non-standardcryptography

According to the comments made in the introduction section, nonstandard picture encryption algorithms are extensively used nowadays, and a lot of research is being done in this field. ProfessorChengqingLietal.divide Chaosbased, DNAencoding, transformationdomain, signal processingin the encryption domain, and Generatingcipher-imagesin other application scenarios are the five core types of non-standard methods. Themostimportantofthesesareasfollows: GeJiao and colleagues suggested a technique for picture encryption based on the

crossdiffusion of two chaotic maps. The keygeneration, which has a bigger security key space than a single one, uses two chaotic sequences, notably the Logistic map and the Chebyshev map.
Furthermore, thesetwosequencesareusedforfurtherimageencryptiondiffusion, which greatly reduces the correlation of nearby pixels [12].
RasulEnayatifarandet al. have developed a fast and secure multiple-image encryption (MIE) technique based on DNA sequences and image matrix indexes. Because theMIEalgorithm considers several pictures, one major worry is the algorithm's speed. Multiple plain-images are joined together to generate a single picture in the first step of this procedure. This picture is then transformed to a one-dimensional array. To permute all of the pixels' positions, half of the array indexes are employed. The sameindexesareassociatedwithDNAsequencetodiffusethe pixelsgreyleveldurringthepermutation[11].

III.PROPOSEDSYSTEM

Theencryptionalgorithm includesthreemajorsteps.The firststepisusedtogeneratethechaoticsequences.Second stepconfused thepixelvalues andthirdstepshuffledthepixel position toproducetherequiredencryptedimage.Letfbean imageofsizeM$\times N$.Thepixeloffisdenotedbyf(i,j),whereiandjisintherangeof1≤i≤Mand1≤j≤N.Now,f(i,j) denotes thegrayvalueatthe pixelposition(i,j) oftheimage f. Theinitialcondition forthelogisticmapisextractedfromthe secretkeyof256bits(32characters) taken inASCIIform denotedas$k = k_1 k_2 k_3 \cdots k_{32}$ (Ki denotesthe8-bitkeycharacterinthei-thkey position).Thevalueoftheinitialconditionforthelogistic mapisgivenby,

3.1 Digital Image Fusion

The stepby step procedure of the algorithm is discussed below.
Step1:TransformtheimageofsizeM×Npixelsintoanarray of $P_i = \{P_1, P_2, P_3 \dots P_n\}$,wherei=1,2,3…n, andn=M×N.Nextconvertthepixelvaluestounsignedintegerintherangeof0 to255usingmodoperation.
Step 2:Generate n numberof chaoticsequence$x_i = \{x_1, x_2, x_3 \dots x_n\}$in the range 0 to 1 using the logistic map mention in Eq. (1) with initialcondition$x_0$andtakingtheparameterr=3.999.Nextconvert$x_i$intounsignedintegerintherangeof0to255usingmodoperation.

Step3:Generatethesequence$C_i = P_i \oplus x_i$ forconfusingthe pixel value. The sign ⊕ indicates bitwise XOR operation.
Step4:Transformthe $C_i = \{C_1, C_2, C_3 \dots C_n\}$toanarray ofsizeM×Ntogettheimagef'.Nextaddonetothe unsigned integersequence$x_i = \{x_1, x_2, x_3 \dots x_n\}$andtransformitintoanarrayof sizeM×Nto getX.
Step5:Finallyexecutethefollowing twostepsforpixel shufflingtogettherequiredencryptedimagef.Herejandk varies from 1 to 255. Thesymbol⇔indicatestheinterchange the values between two pixel positions of f ′.

3.2Standard Encryption

In our system we used Hill cipher as a standard encryption scheme which encrypts the digital fused image to encrypt efficiently.Hill cipher was developed by the mathematician Lester Hill. The core of Hill cipher is matrix manipulations. For encryption, algorithm takesm consecutive plaintext letters and rather of that backups m cipher letters. In Hill cipher, each character is assigned a numerical value. The system can bedescribed as follows

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \qquad \dots (1) \\ C_1 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned}$$

This case can be expressed in terms of column vectors and matrices or simply we can write as

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \qquad \dots (2)$$

C=KP,where C and Pare column vectors of length 3, representing the plaintext andciphertextindependently, and K is a33 × matrix, which is the encryption key. All operations are performed 26mod then. Decryption requires using the antipode of matrix K. The inverse matrix K-1 of a matrix is defined by the equationthen I is e Identity matrix. But the antipode of the matrix doesn't always live, and when it does, it satisfies the equation. K-1 is applied to the ciphertext, and also the plaintext is recovered.
For encryption,

$$C = E_k(P) = K_p \qquad \dots (3)$$

For decryption
Still, there are m 26 different m letters blocks possible, each of them can regarded as a letter in a

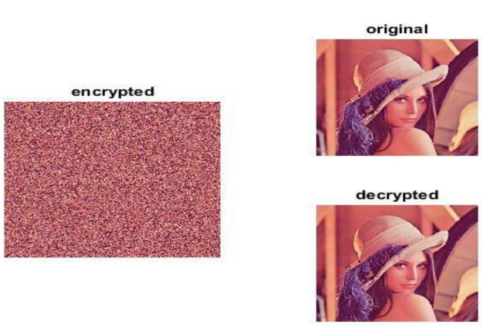
$$P = D_k(C) = K^{-1}C = K^{-1}K_p = P \qquad \dots (4)$$

IV.RESULTS AND ANALYSIS

In MATLAB 2015 a, our approach was simulated, and different parameters were analysed and compared to current algorithms. The analysis' findings are detailed here. Our approach was used to encrypt and decode a variety of photos, which are seen below.

Table 4.1Performance analysis of existing system-digital imagefusion

IMAGE	LENA	JELLY BEANS	HOUSE
ENTROPY	7.7599	6.5835	7.0686



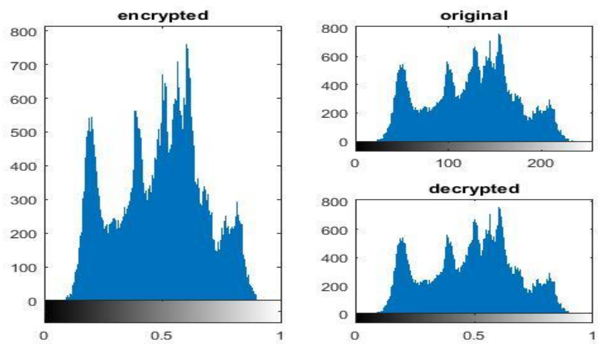
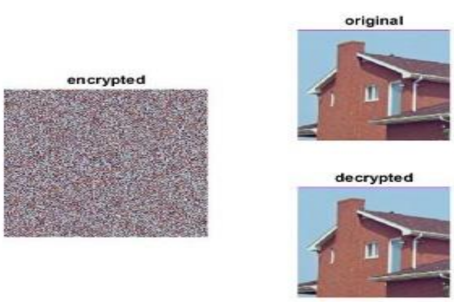


Fig:4.1(a) Encrypted, original and decrypted images of LensFig: 4.1(b)Encrypted, original and decrypted histogram imagesofLena



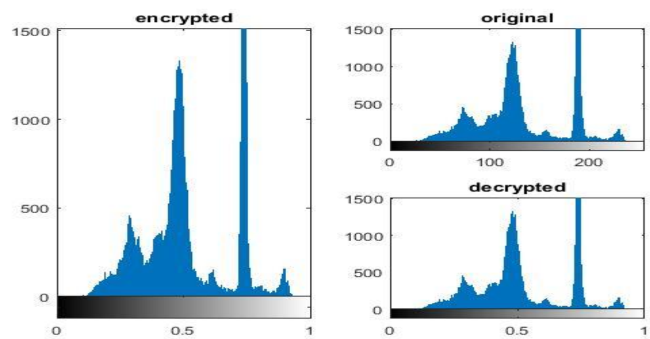


Fig: 4.2(a)Encrypted, original and decryptedimagesofhouse

Fig: 4.2(b)Encrypted, original and decrypted histogram imagesofhouse

Table 4.2Performanceanalysisofproposedsystem–Hybridimage encryption with digital image fusion with hill cipher

IMAGE	LENA	HOUSE
ENTROPY	7.9899	7.9868
MSE	17522	210312
PSNR	5.6949	4.9022
UACI	48.455	53.9360

IV.CONCLUSION

Digital picture security has become more critical for communication across open networks including the internet. The current chaos-based picture encryption techniques have been described and studied in this survey study to confirm their efficacy against various sorts of assaults. To summarise, all of the encryption techniques are beneficial for real-time picture encryption, and each scheme is distinctive in its own manner, making it suitable for various applications. Having numerous chaoticmaps for image encryption may improve security. As a result, encryption, which can be described as a scientific art that is always developing and rapidly expanding, must always demonstrate a high level of security.

ACKNOWLEDGMENT

Thisworkwascarried outby ourcolleaguesMANJU PREETHIB,NARMADHASHRIN,PONSELVIS,under of the guidance of Mr.S.RAJESH KUMAR. We sincerely convey our thanks to our institute for the support during our entire project work. We are also thankful for our beloved Principal, Vice Principal and Head of the Departmentfor the continuous encouragement for precedingourworkinconference.

REFERENCES

[1] BehrouzA.Forouzan,Cryptography&NetworkSecurity,McGraw-Hill press, 2008.

[2] MoatsumAlawida,etal.,Animageencryptionschemebasedon hybridizing digitalchaosandfinite state machine,SignalProcess.164 (2019) 249–266, https://doi.org/10.1016/j.sigpro.2019.06.013 ISSN:01651684.

[3] IslamT.Almalkawietal.AnEfficientDigitalImageEncryptionUsing Pixel Shuffling andSubstitutionforWirelessNetworks.In:2019IEEE JordanInternational JointConference onElectrical Engineeringand InformationTechnology(JEEIT).IEEE,Apr.2019,pp.266–271.ISBN: 978-1-5386-7942-5. doi:10.1109/JEEIT.2019.8717515.

[4] JasonAndress,StevenWinterfeld.TheBasicsofInformationSecurity: UnderstandingtheFundamentalsofInfoSecinTheory andPractice: Second Edition. Elsevier Inc., June 2014, pp. 1–217. ISBN:9780128007440.

[5] AyeshaKulsoomEmailauthorDiXiaoAqeel-ur-RehmanSyedAliAbbas, Anefficientandnoiseresistiveselectiveimageencryptionschemefor grayimagesbasedonchaoticmapsandDNA complementaryrules,in: MultimediaTools andApplications75.1(2016), pp.1-23.

[6] BassemAbd-El-AttyAhmed,A.AbdEl-LatifSalvador,E.Venegas- Andraca,Anencryptionprotocol forNEQRimagesbasedonone-particle quantumwalksonacircle,in: QuantumInformationProcessing,2019. doi:https://doi.org/10.1007/s11128-019-2386-3.

[7] M.Brindha,N.AmmasaiGounden,Achaosbasedimageencryptionand losslesscompressionalgorithm using hashtableandChineseRemainder Theorem,in:Applied SoftComputing40 (Mar. 2016), pp.379–390. doi:10.1016/j.asoc.2015.09.055.ISSN:15684946.

[8] AliBroumandnia,Designingdigitalimageencryptionusing2Dand3D reversible modularchaoticmaps,in:JournalofInformationSecurityand Applications, 2019.doi:10.1016/j.jisa.2019.05.004.ISSN:22142126.

[9] AliBroumandnia,The3Dmodularchaoticmaptodigitalcolorimage encryption,Future Gener.Comput.Syst.(2019), https://doi.org/10.1016/j.future.2019.04.005ISSN 0167739X.

[10]David R.Anderson, Model Based Inference in the Life Sciences:APrimeronEvidence,in:NewYork,NY:SpringerNewYork,2008,pp.51-82. doi:10.1007/978- 0-387-74075-1.

[11]Rasul Enayatifar,FredericoGadelhaGuimaraes,PatrickSiarry,Index- basedpermutation-diffusioninmultiple-imageencryptionusing DNA sequence, in: Optics andLasers inEngineering 115(Apr. 2019), pp.131–140.doi:10.1016/j.optlaseng. 2018.11.017.ISSN:01438166.

[12]X.Peng,G.Jiao,K.Duan,ImageEncryptionwithTheCrossDiffusion ofTwoChaoticMaps,in:KSII TransactionsonInternetandInformation Systems 13.2 (Feb. 2019). doi:10.3837/tiis.2019.02.031. ISSN:19767277.

[13]MengGe,RuisongYe,Anovelimageencryptionschemebasedon3D bitmatrixandchaoticmapwithMarkov properties.In: Egyptian Informatics Journal (2018). doi:10.1016/j.eij.2018.10.001. ISSN:11108665.

[14]LihuaGong, et al., An optical image compression and encryption scheme basedoncompressive sensingandRSAalgorithm,Opt.Lasers Eng. 121 (2019) 169–180, https://doi.org/10.1016/j.optlaseng.2019.03.006ISSN:01438166.

[15] R.Bharathi, T.Abirami," Energy efficient compressive sensing with predictive model for IoT based medical data transmission", Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z

[16] Ramzi Guesmi, et al., Hash key-based image encryption using crossover operator and chaos, Multimedia Tools Appl. 75 (8) (2016) 4753–4769, https://doi.org/10. 1007/S11042-015-2501-0 ISSN: 1380-7501.

[17] S.Kannadhasan, R.Nagarajan and R.Banupriya, Performance Improvement of an ultra wide band antenna using textile material with a PIN diode, Textile Research Journal, DOI: 10.1177/00405175221089690journals.sagepub.com/home/trj