COMPARATIVE SYSTEM OF PRIVACY PRESERVING IMAGE BASED ENCRYPTION

1st Meenu Harikumar
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology,
Palai, Kerala, India
meenuharikumar2001@gmail.com

2nd Navya Sajeev
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology,
Palai, Kerala, India
navyasajeev2001@gmail.com

3rd Sayoojya Saji
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology,
Palai, Kerala, India
sayoojyasaji10@gmail.com

4th Sona Sunny
Dept.of Computer Science and Engineering
St.Joseph's College of Engineering and Technology,
Palai, Kerala, India
sonasunny0963@gmail.com

5th Prof.Thushara Sukumar
Assistant Professor, Department of CSE
St.Joseph's College of Engineering and Technology
Palai, Kerala, India
thusharasukumar@cs.sjcetpalai.ac.in

***Abstract*—Secure data transmission in the virtual world is becoming increasingly difficult. It is due to the activities of hackers on confidential and sensitive information. To avoid hacking at vari- ous levels, there exists a significant number of techniques for data transmission. Cryptography plays a significant role in transferring images securely. A secret key increases the security and complexity of the cryptographic algorithms. The proposed system, will compare the encryp- tion algorithms such as Image Encryption Algorithm Based on Henon chaotic map and Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. This comparison will be performed based on time taken for data encryption and decryption, efficiency in terms of Correlation Coefficient Analysis, Key Sensitivity Analysis, Peak Signal to Noise Ratio(PSNR), Number of Pixels Change Rate(NPCR), Unified Average Changing Intensity(UACI) and Entropy. In this system, the image is an input to encryption to get the encrypted image and then input it to decryption to get the original image. The system could be used for effective image data encryption and key generation, where sensitive and confidential data needs to be transmit- ted along with the image.**

***Index Terms*—Image Encryption, Cryptography, Henon Chaotic Map, Logistic and Two-Dimentional Lorenz**

I. Introduction

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. It is a way of scrambling data so that only authorized parties can understand the information. It is the process of converting human-readable plainimage to incomprehensible image, also known as encrypted image. The use of images and sequences has greatly increased because of the rapid growth of the Internet and widespread use of multimedia systems. While many studies on secure, efficient, and flexible communications have been reported, full encryption with provable security is the most secure option for securing multimedia data. Some traditional encryption algorithms, such as Data Encryption Standard(DES), Advanced Encryption Standard(AES), and Rivest, Shamir, Adleman(RSA) are used in image encryption. However, the traditional encryption algorithm is less efficient when applied to the system that encrypts a large number of pictures. Here we consider two encryption techniques: Image Encryption Algorithm Based on Novel Six-Dimensional Hyper-Chaotic System [2] and Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz [1]. In Image Encryption Algorithm Based on Novel Six-Dimensional Hyper-Chaotic System is a new algorithm for the image encryption/decryption scheme depended on a novel six-dimensional hyper-chaotic system to achieve High level of security, The chaotic sequence generated from system employ for permutation and diffusion the original im- age to create an encrypted image. In Image Encryption Algorithm Based on Logistic and Two- Dimensional Lorenz is a new image encryption algorithm based on two-dimensional Lorenz and Logistic. The encryption test of several classic images proves that the algorithm has high security and strong robustness. It also analyzes the security of encryption algorithms, such as Correlation Coefficient Analysis [4], Key Sensitivity Analysis, Peak Signal to Noise Ratio(PSNR) , Number of Pixels Change Rate(NPCR) , Unified Average Changing Intensity(UACI) and Entropy [8].

DOI: 10.5281/zenodo.8013539

II. Objective and Scope

Cryptography plays a very important role when different users exchange data and information. Users that exchange media files are vulnerable to various security concerns [5]. This includes data leakage and data theft. Usually multimedia contents take up a lot of space. Encryption technique used in the exchange of information should be time efficient. Encrypting the data ensures its privacy in such cases. The objective of this system is to provide evidence of which of the encryption methods has more powerful and effectiveness technique when encrypted file is transmitted, so original file is not available even at the network. So even if any intermediate user sees the data, he will not be able to understand the data. That's why confidentiality and integrity is maintained by this. The proposed system, will compare the commonly used encryption algorithms such as Novel Six-Dimensional Hyper-Chaotic System and Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. This comparison will be performed based on Correlation Coefficient Analysis, Key Sensitivity Analysis, Peak Signal to Noise Ratio(PSNR), Number of Pixels Change Rate(NPCR), Unified Average Changing Intensity(UACI) and Entropy.

III. Literature Review

A. Cryptography

Cryptography is a technique that is widely used to secure data transactions, this technique has also been widely used to secure digital images. Cryptography is a useful technique for encoding data [5]. Cryptography is not only done on text messages, but in multimedia data such as images, audio, and video. Especially in digital images such as medical images desperately need privacy and confidentiality. Cryptography is also widely combined with data hiding techniques like steganography to improve message security. Steganography and cryptography commonly used for securing data transmission. The difference is the way of security, steganography is done by hiding in other media, while cryptography is done by encrypting messages directly to make secured. Some cryptographic techniques that are often used on the image encryption or combined with steganography are a chaotic map, one-time pad etc.

B. Image Encryption

Image encryption [3] is a procedure which converts plain image to an encrypted image by employing a secret key. The decryption process decrypts the cipher image into the original image by employing the secret key. Mainly, decryption operation is like encryption operation but applies in reverse order. The secret keys play a critical role in encryption. Because the security of the encryption approach is mainly dependent on it, two types of keys are utilized, namely, private key and public key. In the private key, the encryption and decryption processes use the same key to encrypt and decrypt the images. In the case of a public key, two keys are utilized, one key for encryption and one for decryption. In this, the encryption key is made public, but the decryption key is always kept private.

C. Entropy

The entropy is a measure of the similarity between the original image and the encrypted-image. The results show that the cover image's entropy and the encrypted image are very closed or similar, which means that the proposed method has a very good visual quality [8]. A plain image does have a value of 'zero' entropy. Consequently, by contraction, such a method of 'zero entropy' image can indeed be modified it into a smaller file size. On the other hand, a high entropy image (i.e., a moon image of intensely derived areas) with a large pixel density cannot be compacted into a smaller image as better as a close to zero image a dissimilar image.

D. Correlation Coefficient Analysis

The correlation between adjacent pixels of the original image is high. The encryption effect can be detected by calculating and comparing the correlation between the original video image and the encrypted video image [4]. . A correlation is a statistical measure of security that expresses a degree of relationship between two adjacent pixels in an image or a degree of association between two adjacent pixels in an image.

E. Key Sensitivity

A highly secure encryption algorithm should be highly sensitive to the key. When the decryption key is slightly different from the encryption key, the encryption and decryption algorithm cannot correctly decrypt the image, and it cannot obtain any original image in the wrong decrypted image. Relevant effective information. The hyper-chaotic maps are sensitive to the initial conditions to a large extent, the proposed technique is highly sensitive to the confidential keys [10]. If a small change in made in encryption key to decrypt the encrypted image, decryption fails completely.

F. Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz

Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz [1], the classical chaotic model is used in the encryption algorithm to generate two sets of chaotic sequences to encrypt the image. The two-dimensional Lorenz chaotic model is used to generate chaotic sequences to encrypt and decrypt the image. In this algorithm, the original image and convert the color image into a grayscale image. The pixel value of grayscale image is converted from decimal to binary representation. Two sets of chaotic sequences is used to scramble the rows and columns of binary representation of grayscale image, and the corresponding decimal image is repre- sented and it is converted from two-dimensional to one-dimensional sequence. Bitwise XOR operation is performed. Convert binary into decimal and convert it into two-dimensional. Then comparison of these encryption techniques that has been carried out on the basis of Correlation Coefficient Analysis, Key Sensitivity Analysis, Peak Signal to Noise Ratio

(PSNR), Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and Entropy.

G. A Fast Image Encryption Using Henon Chaotic Map

Henon map may be stated as a two-dimensional iterated discrete-time dynamical system with a chaotic attractor. Henon chaotic map [2] is a two-dimensional iterated discrete dynamic system that shows chaotic character on specific values of the constants used. Chaotic maps are very sensitive to the initial parameters, i.e., a slight change in the initial conditions drastically changes the overall output generated by the chaotic system. The technique is based upon using chaotic properties of Henon map as pseudo-random number generator along with 128 bit secret key to obtain permutation matrix for shuffling of the original image and a cipher image that is used to finally encrypt the shuffled image. The method is vigorously tested on standard test images based upon various security parameters of digital image encryption. Henon chaotic map along with an externally supplied 128-bit secret key is used to encrypt the original image. After encrypting the image, pixel shuffling is performed using a permutation matrix generated using the chaotic map.

H. A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing

The work done by L. Lidong, D. Jiang, X. Wang, L. Zhang and X. Rong of [7] proposed " A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing". To guarantee the security and high-efficiency of image transmission, a novel triple image encryption scheme based on chaotic system, S-box and image compressing is proposed in this paper. Firstly, the combination process is performed by compressing three plain images to 25 percentage and combining the compressed images with a stochastic matrix. The proposed encryption scheme can be divided into three stages: combination, scrambling and diffusion. In the combination stage, three plain images are compressed by the image compressing technology. Then, the three compressed images are combined with a stochastic matrix generated by a two-dimensional chaotic system. This makes the cipher image dynamic since the parameter of the two-dimensional chaotic system is a dynamic variable which causes the stochastic matrix generated by the chaotic system is different each time. In other words, the generated cipher is different even when it is generated by the proposed encrypt scheme with the identical plain images under the same secret keys, which can resist chosen-plaintext attacks. In the scrambling stage, a novel fast scrambling algorithm named coded lock scrambling is proposed to improve the processing speed. In the last stage, a nonlinear component S-box of which the pseudo-code is demonstrated to participate in the diffusion process.

I. Integral Imaging Based Optical Image Encryption Using CA-DNA Algorithm

The computational integral imaging-based security system, the application of Deoxyribonucleic Acid (DNA) encoding algorithm will cause silhouettes in the cipher image, thereby reducing the security of the system. To solve this problem, a cellular automata-based DNA (CA-DNA) algorithm, which effectively hides the distribution information of the original scene. It can prevent attackers from obtaining any valid information based on the statistical characteristics of the image, which makes our encryption system more security. At the same time, an improved high-resolution reconstruction algorithm is applied to achieve a high-quality decrypted scene. The scheme has high security and robustness. The work done by Y. Wang, X. W. Li and Q. H. Wang of [6] proposed a high security optical encryption approach based on computational integral imaging and CA-based DNA (CA-DNA) encryption algorithm. The high quality random sequences generated by the CA algorithm are used to define which encoding or decoding rules are applied to each pixel of the EIA. Therefore, this algorithm not all pixel coding rules are fixed, which better hides the distribution information of element images. The attacker cannot obtain any valid information based on the statistical distribution of the images, which makes the encryption system more secure. And the CA-DNA complementary operation is applied to further improve the security of the system. Furthermore, a modified computational integral imaging reconstruction algorithm is applied to improve the view quality of the decrypted scene.

J. CFB-Then-ECB Mode-Based Image Encryption

A new encryption mode called CFB-then-ECB [12] is based on a combination of the CFB mode and the ECB mode for AES encryption. Using this new encryption mode, if one encrypted pixel block is noised, this will result in two incorrectly reconstructed pixel blocks during the decryption. This noise spreading is then exploited in a new proposed approach of noisy encrypted image correction. It contains two main steps involving a classifier to discriminate clear and encrypted pixel blocks. After a direct decryption of a noisy encrypted image, the first step is to identify and localize the pixel blocks that are probably incorrectly decrypted. The second step of our proposed approach is to analyze and correct these pixel blocks. Experimental results show that the proposed method can be used to blindly correct noisy encrypted images, while preserving the image structure without increasing the original data size with additional information. Using CFB-then-ECB mode-based image encryption method, an original image is encrypted and then transmitted across a network or stored on a cloud platform. This encrypted image can be noised during its transmission or storage. After a direct decryption, some pixel blocks cannot be correctly decrypted. Moreover, due to the use of the proposed CFB-then-ECB encryption mode, in case of error, there is a noise spreading in the current and the following pixel blocks. This can be exploited in a perspective of noisy encrypted image correction. Consequently, our second contribution concerns the description of a new algorithm of pixel block analysis and noisy encrypted image correction. This proposed method is based on two main steps, namely an initialization step and a correction step. Both of these steps

involve a classifier to discriminate clear pixel blocks from probable incorrectly decrypted ones (i.e which have to be corrected). Indeed, clear and encrypted pixel blocks present different structures and statistical properties, even in the case of very small blocks of 4×4 pixels. By using these differences during the correction process, the content of the original image can be correctly reconstructed.

K. Privacy-Preserving Content-Based Image Retrieval Using Compressible Encrypted Images

A content-based image-retrieval (CBIR) scheme using compressible encrypted images called "encryption-then-compression (EtC) images." The proposed scheme allows us not only to directly retrieve images from visually protected images but to also apply EtC images that can be compressed by using the JPEG standard for the first time. In addition, the sensitive management of secret keys is not required in our framework. The proposed retrieval scheme [17] is carried out on the basis of weighted searching images with MPEG -7-powered localized descriptors (weighted SIMPLE descriptors) combining scalable color descriptor (SCD) or color and edge directivity descriptor (CEDD) . Weighted Simple descriptors are extended, and CEDD is also modified to avoid the influence of image encryption. In an experiment, the proposed scheme is demonstrated to have almost no degradation in retrieval performance compared with conventional content-based retrieval methods with plain images under the use of two datasets. In addition, the proposed scheme is shown to outperform conventional privacy-preserving CBIR schemes including state-of-the-art ones in terms of mean average precision (mAP) scores.For carrying out image retrieval in the encrypted domain, weighted SIMPLE descriptors areextended, and SCD the modified CEDD is used as a globaldescriptor of each patch.

L. Chaotic Image Encryption Scheme With Simultaneous Permutation-Diffusion Operation

A secure and fast chaotic image encryption scheme with simultaneous permutation-diffusion operation is proposed. It combine permutation and diffusion processes into a whole, namely, simultaneous permutation and diffusion operation (SPDO) [20]. This can solve the problem of traditional encryption scheme in which the permutation and diffusion are two independent processes, that leads attackers to crack the two processes separately. In SPDO, the initial value of the current Sine-Sine chaotic map is related to the secret keys and the previous encrypted pixels' values. In this case, the proposed scheme can generate dynamic key streams and indexes that are related to plaintext, which improves the sensitivity to plaintext for the encryption scheme. In addition, the pixel values are processed by row and column (rowlevel and column-level) during the encryption procedure. Thus, the proposed scheme presents lower time complexity and faster running speed compared with bit-level or pixel-level image encryption schemes, which makes the proposed scheme be conducive to the batch transmission and real-time transmission of digital images. The fast image encryption scheme based on SPDO that permute and diffuse the pixel values simultaneously by row and column through Sine-Sine map, which can resist the separated attack. The initial value of the Sine-Sine map is related to the image information and the secret key, which generates distinct keystreams and index sequences for different plain images. The simulation results and security analysis show that can resist common attacks, such as statistical attack, differential attack, chosen plaintext attack and other comprehensive attacks.

M. Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box

The protection of digital content is increasingly becoming a significant issue for researchers and engineers. Here the nonlinear dynamic systems play a vital role in information security through their chaotic behavior and susceptibility to initial conditions. It presents a 3D chaotic map-based symmetric algorithm for multiple images to improve encryption efficiency and encourage secure transmission. The proposed scheme [3] comprises the following four modules: the combination (the images are combined into a single image by merging their color channels); the permutation (using the suggested 3D chaotic map); the S-box generation; and the substitution through the AES substitution method. The proposed algorithm's encryption strength was determined through Entropy, Correlation coefficient, NPCR, and UACI analyses, which were then compared to the past techniques. Furthermore, the proposed method is assessed in terms of its computation time. It demonstrate that it is highly efficient and secure for real-time communication.

N. A Compressive Sensing Based Image Encryption and Compression Algorithm With Identity Authentication and Blind Signcryption

A robust and secure image sharing scheme with personal identity information embedded was proposed based on Compressive Sensing, Secret Image Sharing and Diffie-Hellman Agreement. However, there exists a security flaw in this scheme. It cannot resist the man-in-the-middle attack in the authentication stage. Anyone can disguise himself as a legal person and get the information when exchanging the secret keys, which provides the possibility for information leakage, tampering, and other attacks. In this work [9], proposed an image encryption and compression algorithm with identity authentication and blind signcryption based on Parallel Compressive Sensing (PCS), Secret Sharing(SS) and Elliptic Curve Cryptography (ECC). Firstly, Logistic-Tent system and PCS are employed to complete compression and lightweight encryption in the compression stage. Secondly, random sequences are generated based on Chebyshev map to construct four encryption matrices to perform the encryption process. Meanwhile, the participants' identity authentication and blind signcryption can be achieved by using ECC. Finally, it proves the efficiency and security of the blind signcryption, which

can authenticate the participants identity before restoring the original image. Experiments and security analysis demonstrate that the proposed scheme not only reduce the storage space and computational complexity effectively, but also has resistance against the man-in-the-middle attack, forgery attack and chosen-text attack.

O. Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step

With the growing popularity of digital images in thriving social media and their importance in supporting medical and surveillance industries, the increased security breaches have promoted the need for a practical solution to protect digital image privacy. Chaotic-based S-box image encryption schemes [14] promise to be a practical solution for securing digital images. However, the high-dimensional continuous chaotic has increased the algorithm's complexity. Recent alternatives that focused on double or multiple S-box es approaches, on the other hand, have been proven vulnerable to differential attacks. A chaotic system's intrinsic characteristics, such as pseudo-randomness, instability, and sensitivity to the system's initial conditions and parameters, make the chaotic system have the requisite security conditions. The core principle of chaotic encryption depends on the chaotic framework's capacity to generate a sequence of random numbers that are uncorrelated, similar noise and renewable. It presents an efficient and secure chaotic-based S-box image encryption scheme. Firstly, a single S-box with a size of 10×26 was constructed by using a low-dimensional chaotic system. Without a complex mathematical operation, the constructed single S-box has obvious efficiency advantages and achieved a higher image entropy rate than recent double or multiple S-boxes. Secondly, a new dynamic encryption step method is proposed to solve the high correlation and deterministic problems in multiple S-box encryptions. Under the control of the dynamic encryption step algorithm, it effectively destroys the correlation between the source image pixels.

P. Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Image

A block scrambling-based encryption scheme is presented to enhance the security of Encryption-then-Compression (EtC) systems with JPEG compression, which allow us to securely transmit the images through an untrusted channel provider, such as social network service providers. The proposed scheme [13] enables the use of a smaller block size and a larger number of blocks than the conventional scheme. Images encrypted using the proposed scheme include less color information due to the use of grayscale images even when the original image has three color channels. These features enhance security against various attacks such as jigsaw puzzle solver and brute-force attacks. In an experiment, the security against jigsaw puzzle solver attacks is evaluated. Encrypted images were uploaded to and then downloaded from Facebook and Twitter, and the results demonstrated that the proposed scheme is effective for ETC systems. JPEG standard supports both lossless and lossy compressions, and the encryption schemes are applicable to lossless compression methods. This is because most JPEG compression applications, especially SNS providers and Cloud Photo Storage Services (CPSS), use lossy compression, and lossless compression does not generate any distortion. In order to reconstruct images from encrypted ones, JPEG images downloaded from a provider are decompressed by a JPEG decoder, and then the decryption process is applied to the decompressed images.

Q. Image Encryption Algorithm for Grey and Color Medical Images

Diagnosing diseases using medical images became crucial. As these images are transmitted through the network, they need a high level of protection. If the data in these images are liable for unauthorized usage, this may lead to severe problems. There are different methods for securing images. One of the most efficient techniques for securing medical images is encryption. Confusion and diffusion are the two main steps used in encryption algorithms. S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda [19], presents a new encryption algorithm for encrypting both grey and color medical images. A new image splitting technique based on image blocks introduced. Then, the image blocks scrambled using a zigzag pattern, rotation, and random permutation. Then, a chaotic logistic map generates a key to diffuse the scrambled image. The efficiency of our proposed method in encrypting medical images is evaluated using security analysis and time complexity. The security is tested in entropy, histogram differential attacks, correlation coefficient, PSNR, keyspace, and sensitivity. The achieved results show a high-performance security level reached by successful encryption of both grey and color medical images. A comparison with various encryption methods is performed. The proposed encryption algorithm outperformed the recent existing encryption methods in encrypting medical images. Here, the algorithm for encrypting medical images consists of four stages. In the first stage, we perform image splitting. Confusion (scrambling) is performed in the second stage. The third stage presents key generation based on a logistic map. The final stage presents the diffusion process.

R. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications

Lightweight algorithm encryption technology to protect patients' medical images' privacy. This paper also included different security measurements, encounter parts, and techniques for medical image encryption. Lightweight encryption algorithm [18] develop a secure image encryption technique for the healthcare industry. The proposed lightweight encryption technique employs two permutation techniques to secure medical images. The proposed technique is analyzed, evaluated, and then compared to conventionally encrypted ones in security and execution time. Numerous test images have been used to determine the performance of the proposed algorithm. Several experiments show that the proposed

algorithm for image cryptosystems provides better efficiency than conventional techniques. To secure the medical image, the proposed algorithm is designed carefully to get optimum security. The encryption technique uses three stages to encrypt the image considering 256 bits key value for logical operation.

S. Systematic Survey on Visually Meaningful Image Encryption Techniques

Digital images are widely used in various applications like medical field, military communication, remote sensing, etc. These images may contain sensitive and confidential information. Therefore, images are required to be protected from unauthorized access. The most common technique to protect the images is encryption. In this technique, a secret key and an encryption algorithm are used to change the plain image into an encrypted image. The encrypted image looks like a noisy image and can easily attract the attacker's attention. If an image gets captured and stacked, sensitive information can be revealed. In this regard, Visually Meaningful Encrypted Image [16] technique is developed, which initially encrypts the original image and then hides it into a reference image. The final encrypted image looks like a normal image. Hence, the VMEI technique provides more security as compared to simple image encryption techniques. The VMEI techniques are divided into different categories based on their characteristics. These evaluation parameters are divided into different categories such as security attacks, encryption key attacks, quality analysis, and noise attacks.

T. Encryption Algorithm Based on Novel Six-Dimensional Hyper- Chaotic System

The Encryption algorithm Based on Novel Six-Dimensional Hyper-Chaotic System [11], a new algorithm for the image encryption/decryption scheme depended on a novel six-dimensional hyper-chaotic system to achieve High level of security, the chaotic sequence generated from system employ for permutation and diffusion the original image to create an encrypted image. it is a strong encryption scheme depends on a hyper-chaotic system to enhance security and efficiency. It consists of four stages: chaotic sequence generation, Latin square, permutation, diffusion. The encryption operation utilize Secret key to change over the colored plain image to encrypted image which has random attributes to resist statistical attacks, the plain image is encrypted with Latin square matrix using bit-XOR operation. The stage permutation incorporate scram- bling the locations of encrypted image pixels in a private way, while the diffusion stage include Change the pixel values simultaneously by using bit-XOR operation.

CONCLUSION

The image encryption is widely used to secure transmission of data in an open internet works. Every data has its own unique features, therefore different data requires different type of encryp- tion algorithm. In the proposed System, we compare two image encryption algorithm namely Image Encryption Algorithm Based on Henon Chaotic Map that uses a pseudo-random number generator along with 128 bit secret key to obtain cipher image and next one is Image Encryp- tion Algorithm Based on Logistic and Two-Dimensional Lorenz in which the two-dimensional Lorenz chaotic model is used to generate chaotic sequences to encrypt and encrypt the image. Performance of these encryption method is measured by using Correlation Coefficient Analysis, Key Sensitivity Analysis, Peak Signal to Noise Ratio (PSNR), Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and Entropy.

REFERENCES

[1] T. Li, B. Du and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," in IEEE Access, vol. 8, pp. 13792-13805, 2020, doi: 10.1109/ACCESS.2020.2966264.

[2] S. Ibrahim and A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dy- namic S-Boxes and Elliptic Curve Cryptography," in IEEE Access, vol. 8, pp. 194289- 194302, 2020, doi: 10.1109/ACCESS.2020.3032403.

[3] M. Tanveer et al., "Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box," in IEEE Access, vol. 9, pp. 73924-73937, 2021, doi: 10.1109/ACCESS.2021.3081362.

[4] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu and W. Wang, "A Novel Color Image Encryption Algorithm Based on Three-Dimensional Chaotic Maps and Reconstruction Techniques," in IEEE Access, vol. 9, pp. 61334-61345, 2021, doi: 10.1109/ACCESS.2021.3073514.

[5] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto and M. Doheir, "A Comparative Study of Image Cryptographic Method," 2021, pp. 336-341, doi: 10.1109/ICITACEE.2018.8576907.

[6] Y. Wang, X. -W. Li and Q. -H. Wang, "Integral Imaging Based Optical Image Encryption Using CA-DNA Algorithm," in IEEE Photonics Journal, vol. 13, no. 2, pp. 1-12, April 2021, Art no. 7900812, doi: 10.1109/JPHOT.2021.3068161.

[7] L. Lidong, D. Jiang, X. Wang, L. Zhang and X. Rong, "A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing," in IEEE Access, vol. 8, pp. 210382-210399, 2020, doi: 10.1109/ACCESS.2020.3039891.

[8] M. Tanveer et al., "Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box," in IEEE Access, vol. 9, pp. 73924-73937, 2021, doi: 10.1109/ACCESS.2021.3081362.

[9] X. Li, D. Xiao, H. Mou, D. Lu and M. Peng, "A Compressive Sensing Based Image Encryption and Compression Algorithm With Identity Authentication and Blind Signcryption," in IEEE Access, vol. 8, pp. 211676-211690, 2020, doi: 10.1109/ACCESS.2020.3039643.

[10] Q. Lu, C. Zhu and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," in IEEE Access, vol. 8, pp. 25664-25678, 2020, doi: 10.1109/ACCESS.2020.2970806.

[11] A. Mehdi, Sadiq Ali, Zaydon, "Image Encryption Algorithm Based on a Novel Six- Dimensional Hyper- Chaotic System", 2020, Al-Mustansiriyah Journal of Science, 31. 54. 10.23851/mjs.v31i1.739.

[12] P. Puteaux and W. Puech, "CFB-Then-ECB Mode-Based Image Encryption for an Efficient Correction of Noisy Encrypted Images," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 9, pp. 3338-3351, Sept. 2021, doi: 10.1109/TCSVT.2020.3039112.

[13] T. Chuman, W. Sirichotedumrong and H. Kiya, "Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1515-1525, June 2019, doi: 10.1109/TIFS.2018.2881677.

[14] W. J. Jun and T. S. Fun, "A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step," in IEEE Access, vol. 9, pp. 120596-120612, 2021, doi: 10.1109/ACCESS.2021.3108789.

[15] P. Parida, C. Pradhan, X. -Z. Gao, D. S. Roy and R. K. Barik, "Image Encryption and Authentication With Elliptic Curve Cryptography and Multidimensional Chaotic Maps," in IEEE Access, vol. 9, pp. 76191-76204, 2021, doi: 10.1109/ACCESS.2021.3072075.

[16] V. Himthani, V. S. Dhaka, M. Kaur, D. Singh and H. -N. Lee, "Systematic Survey on Visually Meaningful Image Encryption Techniques," in IEEE Access, vol. 10, pp. 98360-98373, 2022, doi: 10.1109/ACCESS.2022.3203173.

[17] K. Iida and H. Kiya, "Privacy-Preserving Content-Based Image Retrieval Using Compressible Encrypted Images," in IEEE Access, vol. 8, pp. 200038-200050, 2020, doi: 10.1109/ACCESS.2020.3035563.

[18] M. K. Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," in IEEE Access, vol. 9, pp. 47731-47742, 2021, doi: 10.1109/ACCESS.2021.3061710.

[19] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in IEEE Access, vol. 9, pp. 37855-37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[20] L. Liu, Y. Lei and D. Wang, "A Fast Chaotic Image Encryption Scheme With Simultaneous Permutation-Diffusion Operation," in IEEE Access, vol. 8, pp. 27361-27374, 2020, doi: 10.1109/ACCESS.2020.2971759.