
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2022 SCPE. Volume 23, Issues 4, pp. 181–191, DOI 10.12694/scpe.v23i4.2018

HYBRID HYPER CHAOTIC MAP WITH LSB FOR IMAGE ENCRYPTION AND DECRYPTION

S. JAHNAVI *AND C. NANDINI †

Abstract. There are number of images that transmitted through the web for various usages like medical imaging, satellite images, military database, broadcasting, confidential enterprise, banking, etc. Thus, it is important to protect the images confidentially by securing sensitive information from an intruder. The present research work proposes a Hybrid Hyper Chaotic Mapping that considers a3D face Mesh model for hiding the secret image. The model has a larger range of chaotic parameters which are helpful in the chaotification approaches. The proposed system provides excellent security for the secret image through the process of encryption and decryption. The encryption of the secret image is performed by using chaos encryption with hyper hybrid mapping. The hyper hybrid mapping includes enhanced logistic and henon mapping to improve the computation efficiency for security to enhance embedding capacity. In the experiment Fingerprint and satellite image is used as secret image. The secret image is encrypted using a Least Significant Bit (LSB) for embedding an image. The results obtained by the proposed method showed better enhancements in terms of SNR for the 3D Mesh model dataset as 77.85 dB better compared to the existing models that achieved Reversible data hiding in the encrypted domain (RDH-ED) of 33.89 dB and Multiple Most Significant Bit (Multi-MSB) 40 dB. Also, the results obtained by the proposed Hybrid Hyper chaotic mapping showed PSNR of 65.73 dB better when compared to the existing Permutation Substitution and Boolean Operation that obtained 21.19 dB and 21.27 dB for the Deoxyribonucleic Acid (DNA) level permutation-based logistic map.

Key words: Decryption, Encryption, Hybrid Hyper Chaotic map, Least Significant Bit, 3D Mesh model.

AMS subject classifications. 68P25

1. Introduction.

Information security is a part of today's world and images are the common form of multi-media on the internet [1]. Security is one of the significant issues for information transmission through the network [2]. The main aim of the watermarking technique is to perform image information conversion to keep it confidential for the process of encryption by authorized persons [3]. The encryption has the ability for recovering the original data without losing important things in it. Encrypted Secret information is sent through the internet or the wireless networks through the multi-media for a better secure data transmission over distinct communications channels [4, 5]. In the existing research, chaos-based image encryption is utilized that has robust properties with sensitivity, and unpredictability towards the initial dependent conditions [6]. The computational systems are dependent on the internet which utilized watermarking techniques [7]. The Chaos based image encryption has robust properties like unpredictability, and sensitivity towards the conditions [8]. The deterministic conditions in the chaos signify the random behavior with a deterministic system [9].

The existing models have used encryption techniques that includedigital image encryption based on digital image encryption with respect to the random sequences. Digital image encryption is based on the process of image compression coding and the image key. Chaos technology is difficult in cracking the randomness which has made the digital image encryption reliable. Chaos encryption technology refers to the higher dimensional space when proposed by researchers. The researchers faced the problem of encryption and faced difficulty to process the low efficiency of the decryption and encryption process.

. The contributions of the research work are given as follows:

- To develop a hybrid hyper Chaotic Mapping for encrypting the images that consisted of chaos encryption with Enhanced logistic map and henon map.

*Visvesvaraya Technological University, Computer Science and Engineering Department, Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka 560082, India (jahnavishankar.s@gmail.com).

†Professor and Head, Computer Science and Engineering Department, Dayananda Sagar Academy of Technology and Management, India (hodcse@dsatm.edu.in)

- To embed the secret image in a cover image using Least Significant Bit (LSB)for hiding the confidential data on images.

The organization of the research paper is shown as follows. Section 2 explains about literature review of the existing methodologies. Section 3 presents about proposed Hybrid Hyper Chaotic map with LSB for image encryption and decryption. Section 4 illustrates the results and discussion. The conclusion of this research work is given in Section 5.

2. Literature Survey. Ting Luo et al. [11] developed the novel Reversible Data Hiding Method for the 3D Model based on the process of homomorphic encryption. The homomorphic Paillier cryptosystem was used to perform the 3D model encryption. The greedy algorithm was used for data hiding to classify the 3D model vertices that were referred and were embedded to increase the capacity. The embedded vertex has computed based on the reference vertex to predict the module length to generate the prediction error for embedding the data. However, visual quality reduced significantly as the embedding capacity was high.

Wei Zhang et al. [12] developed a CNN-CapsNet for the process of image scene classification for remote sensing. The Capsule network (CapsNet) was used as the proposed model which mainly performs the grouping of neurons as vectors or capsules that replaces with the neuron. The traditional neural network encodes the properties and spatial information of image features achieved equivariance showed an active area for classification. The CapsNet utilizes the capsules or a neuron group or vector that was used for replacing the neuron using a traditional neural network. The spatial properties encode the information of features in an image achieved equivariance showed improvement in the classification. The CNN- CapsNet improved scene classification by using two models such as CapsNet and CNN. The feature maps were used from only one CNN model that was different from retrained CNN

Ferhat Ozgur Catak et al. [13] utilized fully homomorphic encryption and parallel computation for the process of privacy preservation based on biometric data matching. The main aim was to use fully homomorphic encryption based on biometric matching to control the borders. The authentication for the biometric system was performed based on the hash expansion to encrypt the homomorphic features. The homomorphic encryption method showed significant drawbacks with respect to the execution of time. The matching system's deficiency suggested that the model consumed time during fingerprint matching in the encrypted domain. However, the identification of large fingerprint images required computing resources, processing capabilities, and storage.

Wanli Lv et al. [14] developed a Reversible Data Hiding for performing Encryption for the 3D mesh models. The multiple Most Significant Bit (Multi-MSB) was used for reversing the space that was used adaptively for embedding the secret message. The auxiliary information was compressed using arithmetic coding to further free up the redundant space on the 3D mesh models. The developed majority Voting system was the main principle for restoring the mesh model with higher quality. The developed model failed to make data extraction and mesh recovery as they are independent of each other. However, the decrypted cipher text obtained with plain text contained a secret message which could not separate in the clear domain as it failed to perform reversible recovery during data extraction.

Nashwan Alsalam Ali [15] developed a 3D Polygon Mesh Encryption model that maps on3D Lorenz Chaotic Map. The 3D polygon mesh model protects the encryption process using the 3D Lorenz Chaotic map. The developed model provided diffusion better by using an excellent property based on Hausdorff Distance (HD). The histogram metrics were evaluated to adopt them for calculating the matching degree between the original and the extracted model. However, the results were required to be analyzed based on histogram and Hausdorff which encrypted 3D model from different original models.

Xiaojun Lu [16] developed an Adaptive Weight Method to perform the image retrieval using multi-feature fusion. The model used an adaptive weighting method to extract the single feature trust that extracted the unsupervised features. Then, the transfer matrix was constructed based on the trust and the transfer matrix constructed was based on the weight of the single features that are obtained with several iterations. The image decomposition was performed for the process of image classification that considered the image patches achieved results. The key idea behind image decomposition was to perform the process of classifying the image patches. The model extracted a better image description for the retrieval process that showed significance for improving the retrieval performances.

Kaimeng Din et al. [17] developed a Multi-Scale U Shaped Chained M-Shape CNN model to perform

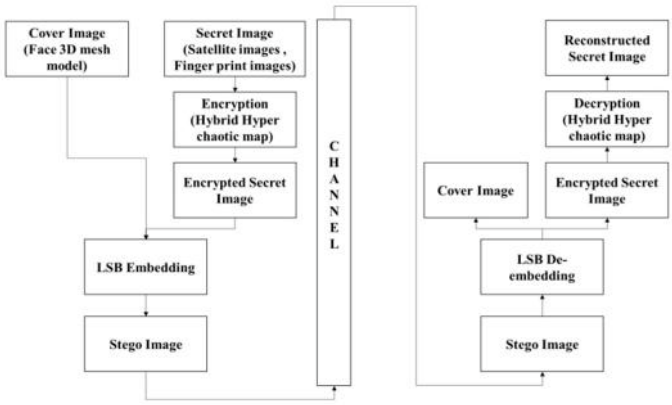

Fig. 3.1: Block diagram of the proposed method

the process of authentication for the generation of high-resolution remote sensing images. The developed model utilized a subject-sensitive perceptual hash function for generating a special case for a conventional hash function. The developed model was based on the subject-sensitive perceptual hash for achieving the CNN architecture extracted the robust features based on the high-resolution Remote Sensing (HRRS) images. Yet, the perceptual hash algorithm used with respect to different resolution images failed to locate tampered areas using deep learning approaches.

Abhimanyu Kumar Patro and Bibhudendra Acharya et al [18] developed a dual-layer cross-coupled chaotic map as an effective model to perform the process of image encryption. The developed model differed from the image encryption schemes multiple times due to two-layered cross coupled chaotic map to perform the process of permutation diffusion operations. The process of left to right flipping, block shuffling, and bit XOR performs the diffusion operation which were carried out in the 1^{st} layer based on the cross coupled chaotic map. Yet, the computational complexity was created in the developed model which was higher compared to the existing models.

Ebrahim Zarei Zefreh et al. [19] developed a hybrid model that consists of DNA computation, chaotic systems, and hash functions for performing image encryption. The developed model performed permutation for the mapping function based on logistic map that was applied for the randomly generated DNA image. The model changed the positions of the elements in the DNA image whichproved the efficiency of the developed scheme. The proposed model analyzed its security and showed improvement in its performance. However, the developed model achieved better security resulting in image encryption schemes that sufficiently showed a faster process for its applications.

Tahir Sajjad Ali and Rashid Ali et al. [20] developed Chaos-based image encryption that consisted of Boolean operation and permutation substitution. Chaotic theory was used to analyze the randomness and unpredictable behaviors of the image encryption process. The Boolean operation and permutation substitution was performed for the RGB components that showed better results for security and analyzing the performances. The model still required security and to be implemented on the real time image for the process of encryption transmission applications.

3. Proposed Methodology. The block diagram of the proposed research is shown in figure 3.1 which consists of a cover image that includes 3D mesh model images and satellite images. The finger print is used to authenticate and improve the security accessing the secret image. At the identification stage, secret image is authenticated by using a biometric identifier.

3.1. UC Merced Land Use Dataset. There are a total of 21 class land-use image datasets used for various purposes. The image has a dimension of 256 $\times$256 pixels that are extracted manually from large scaled

Fig. 3.2: Input images

images from the USGS National Map Urban Area Imagery collection. It is used in various areas from the urban side of the country.

3.2. Sokoto Coventry Fingerprint Dataset (SOCOFing). Sokoto Coventry Fingerprint Dataset (SOCOFing) is a biometric fingerprint database for research purposes. The SOCOFing used 6000 fingerprint images from the 600 African subjects that contained a distinct set of attributes that includes hand, gender, and finger name that are altered synthetically. The versions were provided with 3 different levels of alteration for central obliteration, z-cut, and central rotation, which is shown in Figure 3.2.

3.3. Chaos Encryption with Hybrid Hyper Chaotic Mapping. Once the digital images were collected, the process of encryption of the secret image is performed using the logistic map and henon mapping for performing Chaos encryption for the process of henon map hybridization. Chaos encryption is used extensively for reputation among researchers as it considers the inherent features of the chaos system. The chaos image cryptosystem has two main phases: diffusion and permutation. At the diffusion phase, each of the pixel values are altered and applied with the chaos sequences. The present research performs hyper chaotic mapping for enhancing the digital chaotic maps that are evaluated in terms of chaoticity. The statistical properties have contributed to the chaos based cryptography improvement. The bit reversal approach is used for addressing the issues and the proposed chaotic model modifies the values that are represented with fixed numbers for reversing these fractional bits' order.
With the permutation phase, the permutation for the image pixel positions are performed which overcome the scrambled time over the image without the image pixel value distribution. The diffusion phase and permutation phases used the keys K_i that generated the henon maps and logistic values. The Chaos encryption utilizes the simplest chaotic maps that are called henon map which is mathematically provided in the equation (3.1). The polynomial mapping of two degree uses logistic map that performs chaotic behaviour. The expression for the logistic map is provided in the Eq. (3.1)

$$l_{map}{=}\mu x_n\,(1{-}x_{n-1}) \tag{3.1}$$

where x_n is known as the Chaos sequence that ranges between [0,1] where the term μ is called as the control parameter which is ranging between $(3.57, 4)$.

The Modified Logistic Map's chaotic behavior evaluates the model which highlighted it effectively. The proposed method was analyzed included Bifurcation Diagram (BD), Lyapunov Exponent (LE), Shannon Entropy (SE), Correlation Dimension (CD), Correlation Coefficient (CC), Phase Diagram, and Approximate Entropy (ApEn).

Bifurcation diagram The present research uses Bifurcation diagrams for distinguishing between chaotic and non-chaotic regions. The logistic map showed limited values for parameters that suffered from the periodicity values indicated in unshaded regions.

Lyapunov Exponent (LE) Similarly, the LE is having the desired characteristic for the chaotic map which showed a desirable application under cryptography. The model showed slight changes in the control parameter conditions. The positive LE value is represented the chaotic behavior whereas, the larger LE values show better characteristics using chaotic mapping.

Shannon entropy The metrics that have been used for measuring the randomness in time series are due to chaotic trajectories. Therefore, the chaotic map is evaluated based on the SE that lies in the range of (0,1) that are divided into 210 partitions. The SE calculates the trajectories with the length of 215 that has been used for controlling the parameters. The ideal SE value is equal to 10, which shows higher randomness for a uniformly distributed chaotic trajectory that had visited equal partitions and showed better ergodicity.

Correlation coefficient (CC) The CC is used for measuring the relationship among the chaotic trajectories based on two experimental settings. The CC is used to calculate 2 trajectories that is having the initial conditions at an extreme. These are closer to each other as it has the same control parameters. Thus, the control parameters that are closer to one another starting with trajectories from the initial conditions are considered.

Correlation dimension (CD) The CD is used to observe the geometric complexity of the chaotic attractor that estimates the dimension level for a fractal. The CD measures the attractor with strangeness for the chaotic map. The CD showed a high value which implied a chaotic trajectory that has a phase space moved with the high fractal dimension. The trajectory has lies with the strange attractor that has high irregularity, and unpredictable behaviors that are suitable for cryptography.

Phase diagram The phase diagram reveals more information related to chaotic behaviors which are based on the one map iterations to investigate. The degree of complexity is based on the chaotic attractor that is dependent on the confusion capability with respect to each of the iterations. The entire phase is visited at the space and all these maps are successful in achieving ergodicity. The predictable curve can map the susceptible attacks like a return map to perform the process of signal optimization. The parabolic curve has leaked the information which is used for controlling the parameters for finding the critical points based on the phase diagram.

Approximate entropy The ApEn is used to measure the complexity among the orbits that are generated with distinct chaotic maps. The probability of chaotic orbits has demonstrated a new pattern thatincreases with embedding dimensions. The ApEn values evaluate the same chaotic maps which are set using the distinct parameter has the same bit precision values. The chaotic system showed better values of sensitivity for the initial conditions when the parameter reached 4. The henon map has two dimensional reversible non-linear chaotic maps which were iteration with the point as (x_n, y_n) mathematically expressed as shown in the Eq. (3.2).

$$h_{map}= 1-ax_n^2+y_n, \quad y_{n+1}=bx_n \tag{3.2}$$

From the above Eq. (3.2), $a\epsilon\,(0, 1.4)$, $b\epsilon(0.2,\ 0.314)$ which are known as the control parameters that are working using henon map which is dependent on the parameter values. The logistic and henon map are hybridized five times for accomplishing the transient effect based on the parameter value of the fingerprints as keys represented as K_i. This type of chaotic orbit is obtained from the previous step that is permutated with the diffusion phase on the plane image using Eq. (3.3) and (3.4).

$$x_{n+1}=l_{map}+h_{map} \tag{3.3}$$

$$mim\,(i) = permut\bigoplus K_i(x_{n+1}p\,(i)\,),\ i= 1, 2, 3, \ldots .p\times q \tag{3.4}$$

From the above Equation, p is known as the width and q is known as the height of the plane image, $p(i)$represents the pixel value of an original image, $mim(i)$called as the pixel value of an image. At last,

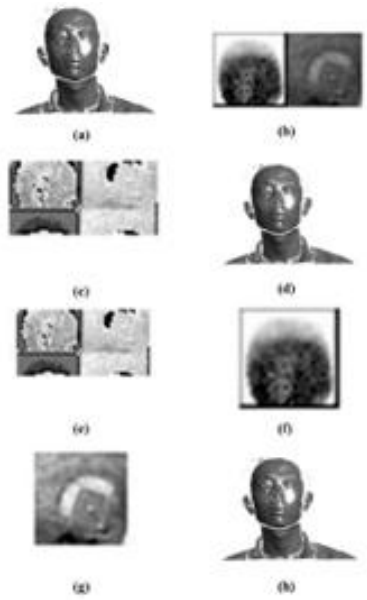

Fig. 3.3: 3D images (a) Cover image, (b) secret image, (c) Encrypted secret image, (d) Stego image, (e) Retrieved image, (f) Reconstructed fingerprint, (g) Reconstructed satellite image, (h) Reconstructed 3D image

the fingerprint image operates with a permutation process which uses an image generated by performing the process of diffusion. It is performed on the permuted image by using the hybrid chaotic model. At the diffusion stage, the output generated is cipher-image that is represented as $c(i)$ mathematically expressed as shown in the Eq. (3.5).

$$c(i) = mim(i) \ , \ i = 1, 2, 3, \ldots p \times q \tag{3.5}$$

3.4. Embedding process and Extraction Process using Least Significant Bit and Decryption Phase. Once the secret image is obtained image in the encryption process, with the cover image transformation, the embedding process is carried out to hide the secret image. The secret image performs the encryption process that considers the cover image transformation to embed the process as it is carried out. The LSB is called the bit operator for the integer positions that embed the unit value. The minimum weighting value is replaced with the sampled image pixels with the binary bits to provide information from the secret data which is hidden inside the pixels. The main purpose is to extract secret information from the locations. Thus, the increase in detection accuracy faces difficulty for the secret data. The pseudo random sequence is used for controlling the location of the secret binary information which is embedded. The LSB model is simple and easy to implement. The model is embedding and extracts the information with a higher rate of hiding capacity faster. The size of the secret image is $m \times n/8$ where the size of the cover image is represented as m×n. The 8 bit LSB has the cover image bit value which is exchanged with the secret image bit value. Thus, the secret image embeds the cover image and the values obtained are binary are converted to the decimal numbers. At the receiver side, the LSB operations are performed on the stego image with the hybrid hyper chaotic mapping. The Chaos decryption with hybrid mapping is performed based on the generated cipher text. The extraction of the secret image was limited with no loss in information and thus the secret image is the same as the original secret image, which is shown in figure 3.3 and 3.4.

4. Results and Discussion. The experimental simulation is performed using a MATLAB (2018a) environment that works with 8 GB RAM, i9 3.0 GHz processor, and 3 TB memory. Mathematical equations of

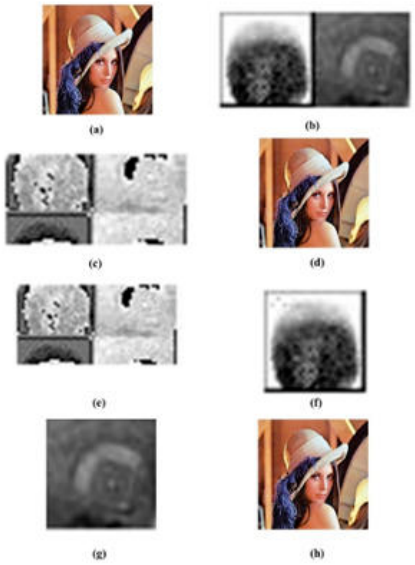

Fig. 3.4: Lena images (a) Cover image, (b) secret image, (c) Encrypted secret image, (d) Stego image, (e) Retrieved image, (f) Reconstructed fingerprint, (g) Reconstructed satellite image, (h) Reconstructed Lena image

entropy value, PSNR, UACI, SSIM, and NCC were indicated in the Eq. (4.1–4.6).

$$E\,(m) = \sum_{x=0}^{m-1} p(m_x) log_2 \frac{1}{p(m_x)} \tag{4.1}$$

where $p(m_x)$ represents the probability of symbol occurrence and m is known as the total number of symbols represented as $m_x \epsilon m$.

$$Peak\ signal\ to\ noise\ Ratio\ (PSNR) = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \tag{4.2}$$

$$Mean\ Square\ Error\ (MSE) = 1/pq \sum_{x=0}^{p-1}\sum_{y=0}^{q-1} [I\,(x,y) - k\,(x,y)\,]^2 \tag{4.3}$$

where p and q are known as the row and the column of an image. $k(x, y)$ is known as the decrypted image, and $I(x, y)$ is known as the original input image.

$$Unified\ Average\ Changing\ Intensity\ (UACI) = \frac{1}{pq} \sum_{x=1}^{p}\sum_{y=1}^{q} \frac{|E_1\,(x,y) - E_2\,(x,y)|}{255} \times 100 \tag{4.4}$$

$$Structural\ SIMilarity\ SSIM\,(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{4.5}$$

$$Normalized\ Cross\ Correlation\ (NCC) = \left[\frac{\sum_{x=1}^{p}\sum_{y=1}^{q} [I\,(x,y)\,k(x,y)]}{\sum_{x=1}^{p}\sum_{y=1}^{q} [I(x,y)]^2}\right] \tag{4.6}$$

Table 4.1: Results obtained by the proposed method for 3D mesh model used as cover image

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Reconstructed 3D	49.008	0.818	0.999	0.171	0.997	0.008
Stego Image	47.635	1.131	0.993	0.324	0.999	0.009

Table 4.2: Results obtained for the existing approaches for performing encryption

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Proposed (Finger print)	99.007	0.002	0.998	0.004	0.995	0.003
Existing (Finger print)	17.617	1127.8	0.577	1.751	0.888	0.242
Proposed (Satellite)	99.008	0.007	0.992	0.003	0.997	0.009
Existing (Satellite)	10.219	6193.2	0.633	4.980	1.090	0.427

Table 4.3: Results obtained for the proposed method

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Without double encryption i.e only logistic method (Fingerprint)	11.964	4136.6	0.743	29.94	1.550	0.355
Without double encryption i.e only logistic method (Satellite)	14.234	2456.8	0.469	1.674	0.809	0.432

Table 4.4: Results obtained for the proposed research work evaluated for different types of datasets such as Fingerprint, Satellite Reconstructed, 3DImg, and Stego 3DImg

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Fingerprint	99.008	0.008	0.994	0.008	0.99	0.005
satellite	99.001	0.001	0.994	0.002	0.997	0.007
Reconstructed 3DImg	49.381	0.752	0.994	0.15	0.995	0.005
Stego 3DImg	48.027	1.026	0.998	0.29	0.992	0.002

where x *and* y is known as the windows from the filter represented as 'k', I is called the original image, σ *and* $\mu$are called as the standard deviation that is having x and$y$ as mean, c_1 *and* c_2 are represented as the constants. $E_1 and\ E_2$ are indicated as encrypted images.

Average Difference (AD) calculates the difference among two adjacent frames on a set of images.

Signal to Noise Ratio (SNR) is defined as the ratio of signal power to the noise power, often expressed in decibels.

4.1. Quantitative Analysis . The proposed method results are compared with the previous researches by comparing with the previous researches that uses reconstructed 3D and Stego image for validating the results.

In table 4.1, the results obtained by the proposed method are shown in terms of PSNR values which are obtained for the reconstructed 3D image. This has obtained 49.008 dB of PSNR values and Stego image of 47.635 dB. The MSE values for the 3D reconstructed image are obtained as 0.818 and 1.131. The value of NCC is obtained as 0.999 and 0.993 for the reconstructed and Stego image. The Average Difference for the reconstructed 3D image is obtained as 0.171 and for that of the Stego is obtained as 0.324.

In table 4.2, the proposed and the existing method logistic are evaluated in terms of PSNR, MSE, NCC, AD, SSIM, and NAE. It is observed that the Proposed system yields better result comapred to exhisting system.

Table 4.3 shows the results obtained for the proposed and the existing methods evaluated in terms of PSNR,

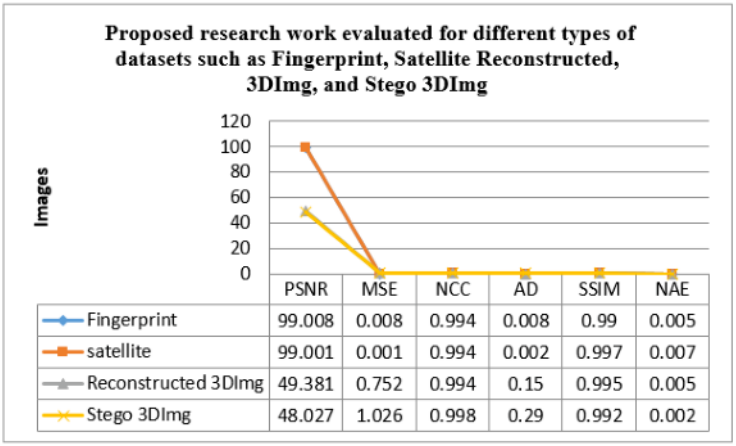

Fig. 4.1: Proposed research work evaluated for different types of datasets such as Fingerprint, Satellite Reconstructed, 3DImg, and Stego 3DImg

Table 4.5: Results obtained by the proposed research work (I)

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Stego Image	65.73	0.02	0.99	0.01	0.99	0.00
Existing (logistic+henon)	29.44	74.04	0.99	0.47	1.00	0.01
Without double encryption (only logistic)	26.33	151.52	0.98	0.94	1.01	0.03

Table 4.6: Results obtained by the proposed research work (II)

Images	PSNR	MSE	NCC	AD	SSIM	NAE
Finger_print (Proposed)	55.77	7.26	0.71	0.31	1.00	0.01
Satellite(Proposed)	59.00	10.00	1.00	0.01	1.00	0.01
Satellite(Existing)	9.95	6588.95	0.66	3.33	0.99	0.45
Fingerprint(Existing)	17.21	1236.69	0.56	0.62	0.91	0.26
Without double encryption (Fingerprint)	8.61	8951.28	0.60	64.93	2.84	0.52
Without double encryption(Satellite)	13.00	3259.43	0.41	43.94	2.57	0.51

MSE, NCC, AD, SSIM, and NAE. The hybrid mapping algorithm consist of Logistc with henon map (as double encryption) and only logistic map as existing systems used for the evaluation of results for both the fingerprint and the satellite images. The Satellite images and the fingerprint images are used for the evaluation of the results of the existing and proposed approaches. The proposed method for fingerprint and satellite images obtained PSNR of 99.007 dB and 99.008dB better when compared to the existing approaches that obtained PSNR of 17.61 dB for fingerprint images and 10.21 dB for the satellite image.

Table 4.4 and figure 4.1 shows the results obtained for the proposed method without double encryption for satellite and fingerprint images. The PSNR values without double encryption uses logistic mapping for encryption, it obtains 11.96 dB and 14.23 dB for the satellite image. The value of MSE for the proposed method without double encryption for the fingerprint image and satellite image is is 4136.6.

Table 4.5 shows the results obtained for the proposed research work which validates the results for various types of datasets such as fingerprint images, satellite images, reconstructed 3D images, and Stego 3D Images

Table 4.7: Results obtained by the proposed research work (III)

Images	**PSNR**	**MSE**	**NCC**	**AD**	**SSIM**	**NAE**
Fingerprint	55.77	7.26	0.71	0.31	1.00	0.01
Satellite	59.00	10.00	1.00	0.01	1.00	0.01
Reconstructed 3DImg	64.35	0.03	1.00	0.01	0.99	0.00
Stego 3DImg	65.73	0.02	0.99	0.01	0.99	0.00

Table 4.8: Comparative Analysis for 2 D images

Authors	**Method**	**PSNR (dB)**	**MSE**
K. Abhimanyu Kumar Patro and Bibhudendra Acharya [18]	Dual-Layer Cross-Coupled Chaotic Map	-	7764.3
Ebrahim Zarei Zefreh [19]	DNA level permutation-based logistic map	21.27	-
Tahir Sajjad Ali and Rashid Ali [20]	Permutation Substitution And Boolean Operation	21.19	497.39
Proposed method	Hybrid Hyper Chaotic mapping	65.73	108.7

Table 4.9: Comparative Results for 3D mesh images

Authors	**Methods**	**SNR (dB)**
Ting Luo [11]	Reversible data hiding in the encrypted domain (RDH-ED)	33.89
Wanli Lv [14]	Multiple Most Significant Bit (Multi-MSB)	40
Proposed	Hybrid Hyper Chaotic mapping	77.85

4.2. Comparative Analysis. Table 4.8 is the comparative analysis of the proposed and the existing models. The values of the PSNR and MSE are validated for existing methods for the standard MATLAB datasets. Table 4.9 shows the results obtained for the 3D mesh model images that are evaluated in terms of SNR (dB).

The existing model Dual-Layer Cross-Coupled Chaotic Map consumed more resources that resulted in 7764.3 MSE values. DNA level permutation based logistic map obtained 21.27 dB of PSNR values due to compatibility of techniques. Also, Permutation Substitution and Boolean Operation obtained PSNR of 21.19 dB and MSE of 497.39 as they used unrealistic requirements. Whereas, the proposed hybrid Hyper Chaotic mapping obtained PSNR of 65.73 dB and MSE of 108.7 of MSE.

5. Conclusion. The present research proposed a highly secured transmission network for real-time world applications. The hybrid map was implemented for ensuring the integrity of the data and the privacy of the secret image. The proposed hybrid hyperchaotic encryption was used for performing encryption of the images based on Chaos encryption with hybrid mapping that consisted of logistic and henon maps. Yet, improvement was required for the direct and indirect recursions which were performed by combining the hybrid chaotic mapping-based encryption technique. Compared to the existing research, the proposed method has used a huge size of images that reduced the time complexity. The results obtained by the proposed method showed better enhancements in terms of SNR for the 3D Mesh model dataset as 77.85 dB better compared to the existing models that achieved Reversible data hiding in the encrypted domain (RDH-ED) of 33.89 dB and Multiple Most Significant Bit (Multi-MSB) 40 dB. Also, the results obtained by the proposed Hybrid Hyper chaotic mapping showed PSNR of 65.73 dB better when compared to the existing Permutation Substitution of

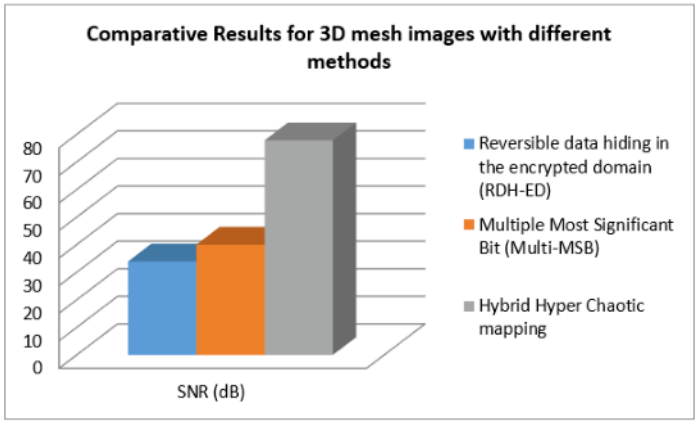

Fig. 4.2: 3D mesh model images evaluated in terms of SNR (dB) of different

21.9 dB and Boolean Operation of 21.27 dB.

REFERENCES

[1] Ali, T.S. and Ali, R., 2020. A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools and Applications, 79 (27), pp.19853-19873.
[2] Gambhir, G. and Mandal, J.K., 2020. Multicore implementation and performance analysis of a chaos based LSB steganography technique. Microsystem Technologies, pp.1-11.
[3] Valandar, M.Y., Barani, M.J., Ayubi, P. and Aghazadeh, M., 2019. An integer wavelet transform image steganography method based on 3D sine chaotic map. Multimedia Tools and Applications, 78 (8), pp.9971-9989.
[4] Younus, Z.S. and Hussain, M.K., 2019. Image steganography using exploiting modification direction for compressed encrypted data. Journal of King Saud University-Computer and Information Sciences.
[5] Mahdi, M.H., Abdulrazzaq, A.A., Rahim, M.S.M., Taha, M.S., Khalid, H.N. and Lafta, S.A., 2019, May. Improvement of Image Steganography Scheme Based on LSB Value with Two Control Random Parameters and Multi-level Encryption. In IOP Conference Series: Materials Science and Engineering (Vol. 518, No. 5, p. 052002). IOP Publishing.
[6] Khan, M., Alanazi, A.S., Khan, L.S. and Hussain, I., 2021. An efficient image encryption scheme based on fractal Tromino and Chebyshev polynomial. *Complex & Intelligent Systems*, 7(3.5), pp.2751-2764.
[7] T. Huynh-The, C.H. Hua, N.A. Tu, T. Hur, J. Bang, D. Kim, M.B. Amin, B.H. Kang, H. Seung, and S. Lee, "Selective bit embedding scheme for robust blind colour image watermarking", *Information Sciences*, Vol. 426, pp. 1-18, 2018.
[8] A.M. Abdelhakim, and M. Abdelhakim, "A time-efficient optimization for robust image watermarking using machine learning", *Expert Systems with Applications*, Vol. 100, pp. 197-210, 2018.
[9] S. Kumar, N. Jain, and S.L. Fernandes, "Rough set based effective technique of image watermarking", *Journal of Computational Science*, Vol. 19, pp. 121-137, 2017.
[10] A. Abbasi, C.S. Woo, and S. Shamshirband, "Robust image watermarking based on Riesz transformation and IT2FLS", *Measurement*, Vol. 74, pp. 116-129, 2015.
[11] Luo, T., Li, L., Zhang, S., Wang, S. and Gu, W., 2021. A Novel Reversible Data Hiding Method for 3D Model in Homomorphic Encryption Domain. *Symmetry*, *13* (6), p.1090.
[12] Zhang, W., Tang, P. and Zhao, L., 2019. Remote sensing image scene classification using CNN-CapsNet. *Remote Sensing*, *11* (5), p.494.
[13] Catak, F.O., Yayilgan, S.Y. and Abomhara, M., 2020. A Privacy-Preserving Fully Homomorphic Encryption and Parallel Computation Based Biometric Data Matching.
[14] Lv, W., Cheng, L. and Yin, Z., 2021. High Capacity Reversible Data Hiding in Encrypted 3D mesh models Based on multi-MSB Prediction. *arXiv preprint arXiv:2110.01010*.
[15] Ali, N.A., Rahma, A.M.S. and Shaker, S.H., 2021. 3D Polygon Mesh Encryption Based on 3D Lorenz Chaotic Map. *iJIM*, *15*, p.103.
[16] Lu, X., Wang, J., Li, X., Yang, M. and Zhang, X., 2018. An adaptive weight method for image retrieval based multi-feature fusion. *Entropy*, *20*, p.577.
[17] Ding, K., Liu, Y., Xu, Q. and Lu, F., 2020. A subject-sensitive perceptual hash based on MUM-Net for the integrity authentication of high resolution remote sensing images. *ISPRS International Journal of Geo-Information*, *9*, p.485.
[18] Patro, K. and Acharya, B., 2021. An efficient dual-layer cross-coupled chaotic map security-based multi-image encryption

system. *Nonlinear Dynamics*, *104*, pp.2759-2805.
[19] Zefreh, E.Z., 2020. An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions. *Multimedia Tools and Applications*, *79*, pp.24993-25022.
[20] Ali, T.S. and Ali, R., 2020. A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. *Multimedia Tools and Applications*, *79*, pp.19853-19873.

Edited by: Vinoth Kumar
Received: Jun 16, 2022
Accepted: Oct 16, 2022