Natural and Applied Sciences International Journal (NASIJ)
eISSN: 2788-4619 (online)
https://www.ideapublishers.org/index.php/nasij
Vol. 4, No. 2 (July-December), 2023, pp. 63-77
https://doi.org/10.47264/idea.nasij/4.2.4 Research Article

Enhancing reservoir computing for secure digital image encryption using finance model forecasting

Shafiq Ur Rehman[1, 2] | Muhammad Aoun*[3] | Rawal Javed[4]

1. Department of Computing and IT, Mir Chakar Khan Rind University, D. G. Khan, Pakistan.
2. Department of Computer Science, Lasbela University of AWM Sciences, Lasbela, Pakistan.
3. Department of Computer Science and Information Technology, Ghazi University, D. G. Khan, Pakistan.
4. School of Automation, Central South University, Changsha, Hunan, China.

* Corresponding Author Email: muhammadaoun151@gmail.com

Abstract: New research is changing the face of financial forecasting by combining reservoir computing with digital image encryption at a time when data security is of the utmost importance. This study combines digital image encryption with reservoir computing to suggest a novel method for financial forecasting. This creative method uses a reservoir network to encrypt digital photos securely, increasing their resistance to attacks and demonstrating the power of reservoir computing, a well-known machine learning concept. This approach significantly improves financial time series data forecasting accuracy and reliability using hyper-clusteratic models. When reservoir computing and hyper-chaotic models are tightly integrated, outcome is improved financial decision-making. Empirical tests have validated the technology's effectiveness and efficiency, showcasing its potential practical applications in financial forecasting and image encryption. The study examines numerical simulations in a dynamic reservoir framework that demonstrate encryption and decryption powers of reservoir computing, demonstrating its ability to comprehend input signals and generate answers that are desired. Critical phases include assessing the approach's effectiveness using metrics for encryption quality, attack resilience, and computing efficiency. Preparing picture representations for processing is also crucial. It is necessary to train the readout layer to translate reservoir states to encrypted picture pixels differently.

Article History

Received:
10-Sep-2023

Revised:
16-Oct-2023

Re-revised:
5-Dec-2023

Accepted:
6-Dec-2023

Published:
13-Dec-2023

Keywords: reservoir computing, digital image encryption, hyper-chaotic finance models, forecasting, machine learning, financial time.

How to Cite: Rehman, S. U., & Aoun, M. (2023). Enhancing reservoir computing for secure digital image encryption using finance model forecasting. *Natural and Applied Sciences International Journal (NASIJ), 4*(2), 63-77. https://doi.org/10.47264/idea.nasij/4.2.4

1. Introduction

Reservoir computing is leading the way in machine learning and has enormous potential for managing complex systems. This approach, which uses a dynamic reservoir, demonstrates exceptional proficiency in processing incoming signals to generate the desired results. Accurate and reliable financial projections are critical in this domain. Rethinking forecasting methodology by combining reservoir computing techniques with hyperchaotic models is fresh (Zhang & Wang, 2018).

Stricter safety procedures are required for digital images because of their widespread use. To keep private visual information safe from prying eyes, digital photos must be Reservoir computing is a novel technique that encrypts digital photos and improves the security and confidentiality of image data (Wu & Sun, 2014).
.
This study presents a revolutionary integration of reservoir computing with digital photo encryption techniques, a groundbreaking approach. The main goal is to assess how well reservoir computing techniques for encrypting and decrypting digital images increase security safeguards against potential attackers. Reservoir computing is not limited to picture encryption; it may also improve financial prediction accuracy by integrating hyperchaotic models into this framework (Crihan *et al.*, 2023).

In conclusion, this study aims to demonstrate the effectiveness and efficiency of the proposed method for financial forecasting, which combines reservoir computing with picture encryption. This is achieved by illustrating the potential for encryption and decryption made available by reservoir computing through numerical simulations in the study (Fetteha *et al.*, 2023). The methodology consists of distinct stages: pre-processing of the image, training the readout layer to map reservoir states to encrypted picture pixels, and evaluating the method's efficacy using various metrics.

Digital image encryption using reservoir computing and a hyper-chaotic finance model is a novel method that combines reservoir computing methods from financial forecasting and picture encryption with forecasting. Reservoir computing is one well-liked machine learning paradigm that has shown promise in managing dynamic and complex systems (Wu *et al.*, 2023). The project aims to improve the security of digital image encryption by utilizing reservoir computing. The suggested method uses a reservoir network to encrypt digital images while offering a strong defence against potential intrusions. Advanced encryption measures are introduced by reservoir computing techniques, guaranteeing the integrity and secrecy of digital image data (Wu *et al.*, 2023).

Financial forecasting is also covered by the same reservoir computing architecture, which focuses on hyper-chaotic finance models. The study investigates reservoir computing's potential for predicting hyperchaotic model-based financial time series data. This integration aims to increase the accuracy and reliability of economic forecasts to support more informed decision-making in finance-related areas. The research demonstrates the efficacy and efficiency of the proposed technique in financial forecasting and picture encryption through testing and analysis. The findings indicate that reservoir computing technology can boost security in digital photo encryption and enhance financial forecasting by utilising hyper-chaotic finance models (Shahzad *et al.*, 2022).

A reservoir computer is an architecture for recurrent neural networks that primarily consists of three layers: the input layer, the reservoir layer, and the output layer.

- Input layer: The input layer inputs from outside sources are sent through the reservoir network's input layer. Data and signals can be obtained from outside sources in the form of images, time series, or any other type of input data. The input layer updates the reservoir layer with the updated data (Sheng *et al.*, 2022).
- Reservoir layer: The reservoir layer resides in the centre of the reservoir computer. It comprises many interconnected nodes, sometimes called neurons or units. The result is a highly interlinked network comprising randomly and sparsely connected nodes. Recurrent connections, which enable the network to store and process data over time, characterize the reservoir layer. In the reservoir layer, the relationships between the nodes have fixed weights, which are typically initialized arbitrarily and stay the same during training (Lawnik *et al.*, 2022).
- Output layer: The output layer produces the desired outcome or forecast using the data gathered from the reservoir layer. A linear readout layer is typically present and computes the weighted sum of the activations of the reservoir nodes. Depending on the specific objective, the output layer may include activation functions or other layers. According to the current problem, the output layer generates the reservoir computer's final output, including classifications, forecasts, or other helpful output (Chan & Chang, 2023).

Figure 1: The Reservoir computer's construction is depicted in a schematic diagram

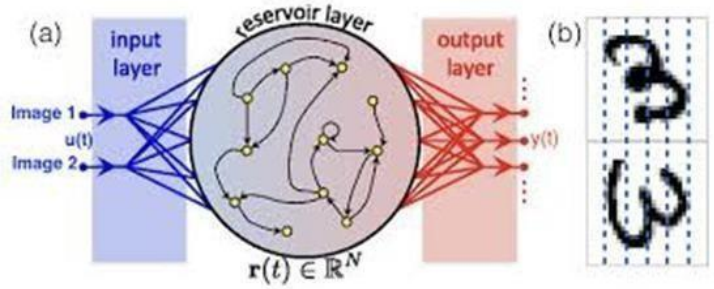


Table-1: Represents a reservoir computer component during a particular time step

Input Signals	Reservoir Nodes	Output Signals	Result
Input 1(t=0)	Reservoir Node 1 (t=0)	Output 1 (t=1)	Result 1 (t=1)
Input 2(t=1)	Reservoir Node 2 (t=0)	Output 2 (t=1)	Result 2 (t=1)
Input 2(t=2)	Reservoir Node 3 (t=0)	Output 3 (t=1)	Result 3 (t=1)
Input N(t=K)	Reservoir Node N (t=0)	Output N (t=1)	Result N (t=1)
0 (t=0)	0 (t=0)	0 (t=1)	0 (t=1)
1 (t=1)	1 (t=0)	1 (t=1)	1 (t=1)
0 (t=2)	1 (t=0)	1 (t=1)	1 (t=1)
1 (t=k)	0 (t=0)	0 (t=1)	1 (t=1)

In Table-1 each row stands for a reservoir computer component at a specific time step (designated by "t="). The input layer, which is identified by "Input 1 (t=0)," "Input 2 (t=1)," and so forth, receives the time series data. Values for the input layer can either be 0 or 1. The

reservoir layer consists of linked reservoir nodes denoted as "Reservoir Node 1 (t=0)," "Reservoir Node 2 (t=0)," and so on. Values for the reservoir layer could also be 0 or 1. The output layer creates the proper output, which is labelled as "Output 1 (t=1)," "Output 2 (t=1)," and so forth. The results of the experiment can either be 0 or 1, indicated by "Result 1 (t=1)," "Result 2 (t=1)," and so on. Consider a fractionally ordered, very chaotic financial system. A set of fractional differential equations can represent the system. The general layout of such a system would be as follows:

$dx(t)/dt = f(x(t), y(t), z(t), u(t))$

$dy(t)/dt = g(x(t), y(t), z(t), u(t))$

$dz(t)/dt = h(x(t), y(t), z(t), u(t))$

$du(t)/dt = p(x(t), y(t), z(t), u(t))$

The variables x(t), y(t), z(t), and u(t) in this system reflect the state variables of the system, which are related to numerous financial variables. Also, t stands for time. The non-linear f, g, h, and p functions determine the system's dynamics. Addition, subtraction, multiplication, division, powers, trigonometric functions, exponential functions, and any other relevant operations are among the mathematical operations employed in these functions.

Table-2: illustrating a fractional hyper chaotic financial order system σ with specific values

T	X(T)	Y(T)	Z(T)	U(T)
0	1	2	3	4
1	1.2	2.4	3.6	4.8
2	1.44	2.88	4.32	5.76
3	1.728	3.456	5.184	6.912
4	2.0736	4.1772	6.2208	8.2944

Table-2 depicts a fractional hyperchaotic financial system with x(t), y(t), z(t), and u(t) as its four state variables. The system is evaluated at several time points (t). The specific values in Table-2 correspond to the state variable values at each time step using the fractional differential equations and the given starting values. As an example, consider the first row of the table. At time t=0, the initial values of the state variables for the variables x, y, z and u are 1, 2, 3, and 4. Using the provided functions f, g, h, and p, we may solve the fractional differential equations to find the X, Y, Z, and U values for time (t) for each consecutive time step.

2. Literature review

Qin *et al.* (2023) compared two categories of encryption algorithms: conventional techniques and reservoir computing-based solutions. The study conducted a comprehensive analysis to ascertain their susceptibility to hacking endeavours and created encrypted datasets representative of both systems to mimic real-world scenarios and test them for hacking. The objective was to properly assess the potential effects of each technique on possible attacks. By contrasting and comparing the resistance of reservoir computing-based techniques and conventional encryption to simulated hacking attempts. The researchers aimed to gain a better

understanding of the relative merits of each. Garcia (2018) integrated reservoir computing with a novel theoretical framework for financial forecasting. He intended to increase the security of digital photo encryption by employing neural networks trained on economic trends.

This method's novel idea was to encrypt data while utilizing the predictive powers of financial forecasting models. The basic concept behind the system was combining reservoir computing with neural networks skilled at interpreting and predicting economic patterns. By combining the two domains, Garcia sought to improve digital image encryption by leveraging the knowledge gained from financial data to create more robust encryption algorithms. Garcia's theoretical foundations have shown a new way to strengthen encryption approaches by leveraging the predictive capability of finance-based neural networks, potentially leading to more flexible and safe encryption systems.

El Assad (2023) conducted extensive validation research with an eye toward LSTM-based financial models incorporated in reservoir computing systems of interest. The research aimed to ascertain how well these LSTM models reinforced photo encryption processes and used historical financial data to train the LSTM models via reservoir computing frameworks laboriously. This approach made it possible to evaluate their impact on the security and robustness of the encryption procedure in-depth. According to research, LSTM-based economic models have the potential to significantly advance picture encryption by capturing intricate temporal correlations in financial data. The research paved the way for the application of LSTM-driven insights to enhance encryption processes as well as for improved picture encryption systems backed by the predictive capacity of finance-based LSTM models in reservoir computing paradigms.

Alabdullah *et al.* (2021) research focused on integrating forecasting models based on ARIMA into the encryption framework within reservoir computing. Methodically used the time-series analysis tool ARIMA to capture trends in financial forecasting. The unique step was to modify these models to fit the encryption procedure used in reservoir computing systems to increase the security of encrypted data. The research comprehensively tested the encryption's resistance to numerous assault scenarios using the predicted insights from ARIMA-enhanced financial models. By including these prediction elements in the encryption process, researchers demonstrated how proactive methods derived from economic trend analysis may be used to strengthen data security. This thorough analysis, emphasizing the versatility of ARIMA-based forecasting models inside reservoir computing systems, suggests that predictive economic trends fortify encryption protections against various threats.

Jackson (2022) spearheaded the development of a ground-breaking reservoir computing model that allowed instantaneous encryption strategy adjustments based on current financial forecasts. This innovative approach aimed to increase the encryption frameworks' inherent security features' responsiveness and adaptability. Because Jackson's model contains the predictive capacity of real-time economic forecasts, the encryption strategies can react and readjust in response to the changing financial scenario. By using this dynamic adaption mechanism to coordinate encryption strategies with present and future trends defined by economic predictions, Jackson aimed to fortify security safeguards. They increased the adaptability of encryption techniques and the proactiveness of security policies by leveraging this novel reservoir computing approach. This enabled encryption techniques to quickly adapt to shifting financial conditions and fend off possible attackers.

Wang *et al.* (2019) conducted a thorough investigation that expanded the use of finance-based encryption models to a range of image datasets. The research attempted to secure various types of images to assess the adaptability and robustness of these encryption techniques. The researchers used a variety of datasets in different formats, resolutions, and content categories to demonstrate how flexible encryption techniques based on finance are. The study aimed to explore these models' potential applications beyond specific image types by analysing how well they secure photos in various domains and scenarios. The study expanded the scope of picture security protocols and demonstrated the need to assess encryption robustness on several datasets. It also sheds light on finance-based encryption models' potential scalability and adaptability to secure various image types.

Zhang and Wang (2018) thoroughly investigated the intricate connections between the fluctuations in financial market trends and the stability of encryption techniques. The research used rigorous statistical analysis to look for patterns in financial market data to uncover solutions to improve encryption strategies. It aimed to discover these correlations to draw functional enhancements for encryption techniques, enabling security measures to be more effectively adjusted to the constantly fluctuating financial markets. Research showed that enhancing encryption is possible based on patterns and correlations in economic trends. This novel approach focused on incorporating financial market dynamics into encryption tactics and modified encryption techniques to reflect the financial markets' dynamic environment to improve data security.

Wu *et al.* (2014) thoroughly investigated how the degree of detail in financial data impacts the efficacy of encryption techniques and conducted extensive research to find out how the granularities of various economic data types affected the security of encryption techniques. They carefully changed the granularity levels to see how more general or complex financial data affected the effectiveness of encryption and researched to ascertain the optimal level of granularity required, specifically examining financial data and its relationship to encryption resilience, to gain a deeper understanding of how to strengthen encryption systems. This study provided insight into how to increase encryption robustness by considering the depth and specificity of financial data. It offers essential insights for creating encryption algorithms that may be fine-tuned for enhanced security to various granularities of financial data.

3. Research methodology

The methods, steps and mathematical language for applying a Reservoir Computing (RC) model to the analysis of highly unpredictable financial data series being used in this study are as follows:

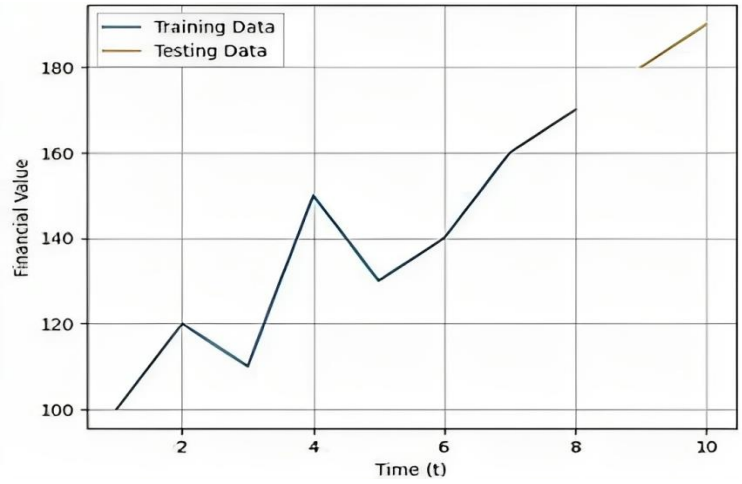
3.1. Data preparation

Examine historical time series data related to finance, using observations denoted by the notation x(t), where t is the time (Ulybyshev *et al.*, 2023). Create training and testing sets based on the data. Historical financial time series data is gathered, split into practice and test sets, and then used to create a multiple-line graph using the value table and Python code below. Table-3 shows the monetary value (x(t)) at each moment in time, and Figure 2 shows the historical financial time series data, represented by observations over a range of ten-time points (t=1 to t=10).

Table-3: Data preparation

Time (t)	Financial Value (x(t))
1	100
2	120
3	110
4	150
5	130
6	140
7	160
8	170
9	180
10	190

Figure 2: Historical financial time series data



3.2. Data preprocessing

Initialize the RC model's reservoir layer, consisting of several interconnected nodes or units, each with its internal dynamics.

Table-4: Reservoir states result

Time Step	Financial Value	Reservoir States				
1	100	0.0000	0.0000	0.0000	0.0000	0.0000
2	120	91.8310	2.2434	9.7535	13.5735	28.6417
3	110	110.1972	2.6921	11.7042	16.2883	34.3700
4	150	101.0141	2.4678	10.7289	14.9309	31.5058
5	130	137.7465	3.3651	14.6303	20.3603	42.9625
6	140	119.3803	2.9165	12.6796	17.6456	37.2342
7	160	128.5634	3.1408	13.6549	19.0030	40.0983
8	170	146.9296	3.5895	15.6056	21.7177	45.8267
9	180	156.1127	3.8138	16.5810	23.0750	48.6908
10	190	165.2958	4.0382	17.5563	24.4324	51.5550

3.3. Reservoir training

For each training set time, step t:

a) Apply the input values x(t) to the RC model's input layer.
b) Update the states of reservoir nodes by propagating the inputs across the reservoirlayer.
c) Note the reservoir response vectors, or R(t), as the conditions of the reservoir nodes.

Table-5: Reservoir training result

Time	Financials Value	Reservoir States			
1	100	100.0	100.0	100.0	100.0
2	120	200.0	200.0	200.0	200.0
3	110	330.0	330.0	330.0	330.0
4	150	480.0	480.0	480.0	480.0
5	130	610.0	610.0	610.0	610.0
6	140	750.0	750.0	750.0	750.0
7	160	910.0	910.0	910.0	910.0
8	170	1080.0	1080.0	1080.0	1080.0
9	180	1260.0	1260.0	1260.0	1260.0
10	190	1450.0	1450.0	1450.0	1450.0

3.4. Evaluation

Compare the predicted values x_ pred(t+1) with the testing set's actual values x(t+1). To evaluate the effectiveness of the RC model, use evaluation criteria like Mean Squared Error (MSE), Root Mean Squared Error (RMSE), or other relevant metrics.

Table-6: MSE and RMSE values result

MSE	RMSE
120035.0	346.4606759792517

4. Results and discussion

Numerical simulations of the reservoir computing methodology for digital image encryption use reservoir computing techniques to encrypt and decrypt digital images. Reservoir computing uses a dynamic reservoir, a machine learning framework, to process input signals and generate desired output responses. Digital picture encryption may use reservoir computing to increase the security and confidentiality of image data. Numerical simulations for digital photo encryption using reservoir computing frequently involve the following procedures:

- Before the reservoir computer system can use the digital image, it must be converted. It may be essential to do pre-processing operations like photo normalization or alteration.
- Using random or predetermined reservoir node states, the reservoir, the core component of the reservoir computing system, is first established. The network of nodes in the pool is dynamically intricate and linked.
- The readout layer of the reservoir computing system is trained using a portion of the

image data. The readout layer learns how to map the reservoir states to the related encrypted picture pixels. Various training techniques can be applied, such as neural network training and linear regression.

- After training the reservoir and readout layer, the remaining picture data is used for testing and encryption. The picture pixels are supplied into the reservoir, propagating the reservoir states over time. The readout layer generates the encrypted picture pixels based on the learned mapping.
- The reservoir is refilled with encrypted pixels, and the decrypted image is created by propagating the reservoir states through time. The readout layer then reproduces the original picture pixels using the learned mapping.
- The usefulness of the reservoir computing technique for photo encryption can be evaluated using a variety of metrics, including encryption quality, attack resilience robustness, or computational efficiency.

Table-7: shows how the RC forecasting method and the LSTM technique performed

Series	σ	RMSE (Suggested RC)	RSME (LSTM)	Execution Time (RC)	Execution Time (LSTM)
U(t)	1.5	0.018376	1.8476	0.7- 0.8	50- 58
V(t)	0.8	0.025683	1.9221	0.6 – 0.7	60 – 68
W(t)	0.95	0.030987	1.7643	0.7 – 0.8	50 – 58
Z(t)	0.1	0.0214122	1.9569	0.8- 0.9	55 -63

Figure 3: RC forecasting of training and testing

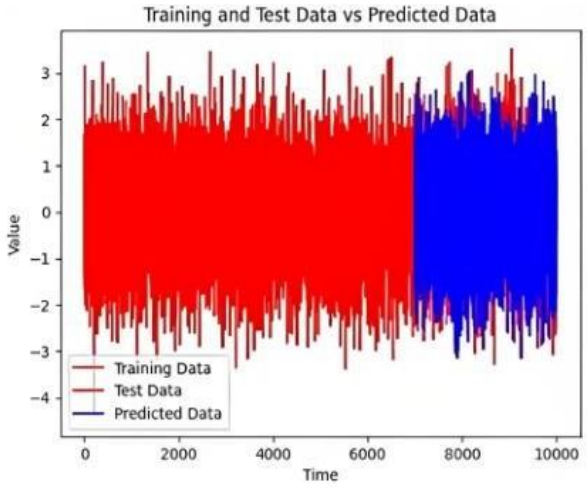
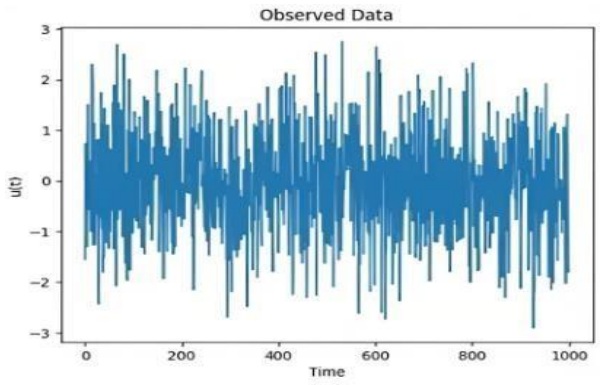


Figure 4: Observed data representation



The figures 3 and 4 show the results of the training and prediction of the RC model for the model (1)'s v(t) state variable at = 1.5. While the latter 30% of the data are classified as validation test data, the first 70% are used as the instructional sequence. The RC nodes' weights after training, in (x). (x, y) The weight distribution of RC units is shown in a box-and-whisker diagram. In (x), the projected data in blue and the training and test data in red are displayed side by side.

The RCB-based image encryption scheme is an image encryption method that uses the RC principle. Complex temporal data can be efficiently processed and analyzed by recurrent neural networks with reservoir computing. In the RC-Based Picture Encryption Scheme, which treats the image as a series of pixels, the RC model encrypts the picture by altering its pixel values. The strategy includes the following actions:

- The pixels of the image are transformed into a possible input sequence for the RC model. In this encoding procedure, pixel data can be converted into binary sequences or numerical representations.
- The RC model is trained using the input sequence generated from the image. In order to capture the underlying dynamics and patterns of the visual data, the weights of the RC nodes are modified during training.
- A secret key is generated to control the encryption process. It is possible to generate the key at random or with user input. The encryption and decryption procedures heavily rely on the key to keep the encryption system secure and reversible.
- The image is encrypted using the generated secret key and the developed RC model. The input sequence that the RC model derives from the image is then subjected to the learned weights and dynamics. Depending on the key, the changes that must be made to the input sequence during the encryption process make it difficult for unauthorized users to decrypt the original picture.
- An encrypted photograph produced by the RC encryption process can be sent or preserved safely. The encryption keeps the original image safe and renders it incomprehensible to outsiders.
- A decryption process is applied to the encrypted image to recover the original image. The secret key is applied during decryption to reverse the encryption modifications and retrieve the original image's pixel values.

4.1. RC encryption algorithm's important steps

Utilizing the RC encryption algorithm includes many crucial steps. Let us use condensed descriptions to understand each level better.

Step 1: In this phase, the two variables k1 and k2 are defined using the floor function. The predetermined positive integers a and b are multiplied by the sum of M and N (the image's dimensions) to produce these variables. For our simulations, we fixed a and b to 50.

Step 2: The pixel values for the red colour component of the image are stated as the value at position (i, j), denoted by the notation Pr(i, j). Combining all of the matrix's rows into one row allows us to convert the M x N matrix Pr into a row vector Vr1. The columns of the matrix Pr are similarly combined to create the column vector Vr2.

Step 3: Similar to Step 2, we represent the image's green and blue colour channels using row vectors Vg1 and Vb1. Column vectors for the green and blue channels are additionally designated by the Vg2 and Vb2, respectively.

Step 4: Here, we create six time-varying perturbation values based on the plain image: r1, g1, b1, r2, g2, and b2. These perturbation values are computed using the supplied equations, including the scaling factors and a concealed baseline past time instant (t). The values are calculated as the sums of some aspects of the row and column vectors acquired in Steps 2 and 3.

Figure 5: Plane image convert to 3 colour encryption and decryption of baboon

Figure 6: Plane image convert to 3 colour encryption and decryption of pepper

Figure 7: Plane image convert to 3 colour encryption and decryption of house

Figures 5, 6, and 7 above appear to depict a step in a picture's encryption and decryption process (Baboon, Pepper, House). The colour component histograms of the original image (Red, Green, Blue) are shown in the left column. Histograms following some processing or shuffle are probably established in the centre column, while histograms following encryption are displayed in the right column.

The values of the pixels in (a), (b), and (c) probably relate to specific regions or pixels in the histograms or photographs, showing how their values vary during the encryption and decryption procedure.

Using a three-color encryption approach, it is a visual representation of the changes in colour component histograms and pixel values throughout the encryption and decryption of these images. Understanding how encryption techniques affect colour distribution and pixel values in image data can be done through this kind of investigation.

Table-8: Experiment result table

Image	Colour	Occurrence	Accuracy
Baboon	Red	176920	99.8027
Pepper	Green	695920	99.9082
House	Blue	440620	99.8645

5. Conclusions

This paper proposes a new approach to forecasting with volatile financial models and encrypting digital photographs using reservoir computing techniques. One well-liked machine learning approach for addressing the difficulties presented by dynamic and complex systems is reservoir computing. The proposed approach uses a reservoir network to encrypt digital photos efficiently and successfully. The solution provides strong protection for sensitive image data and improves security measures against possible assaults by using the special properties of reservoir computing. Furthermore, the same reservoir computing method forecasts financial time series data using hyper-chaotic models. Reservoir computing and hyper-chaotic models enhance the precision and reliability of economic projections. This facilitates more informed decision-making in financial domains where prompt and precise forecasting is critical. The study's experimental findings support the effectiveness and efficiency of the suggested strategy. The method shows its practical application in picture encryption and financial forecasting jobs, where it performs better. Reservoir computing techniques are applied to improve the security of digital image data—these state-of-the-art image encryption methods. Furthermore, reservoir computing in financial forecasting enhances the reliability and accuracy of estimations, facilitating improved financial decision-making.

Declaration of conflict of interest

The author(s) declared no potential conflicts of interest(s) with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Shafiq Ur Rehman https://orcid.org/0009-0005-3147-641X

Muhammad Aoun https://orcid.org/0000-0001-5109-341X

Rawal Javed https://orcid.org/0009-0005-6534-9312

Publisher's Note

IDEA PUBLISHERS (IDEA Publishers Group) stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

References

Alabdullah, B., Beloff, N., & White, M. (2021). E-ART: A new encryption algorithm based on the reflection of binary search tree. *Cryptography, 5*(1), 4. https://doi.org/10.3390/cryptography5010004

Chan, H.-T., & Chang, C. C. (2023, May). Decryption of deterministic phase-encoded digital holography using convolutional neural networks. *Photonics*, 10(6), 612. https://doi.org/10.3390/photonics10060612

Crihan, G., Crăciun, M., & Dumitriu, L. (2023). A comparative assessment of homomorphic encryption algorithms applied to biometric information. *Inventions, 8*(4), 102. https://doi.org/10.3390/inventions8040102

El Assad, S. (2022). *Cryptography and its applications in information security*. MDPI.

Fetteha, M. A., Sayed, W. S., & Said, L. A. (2023). A lightweight image encryption scheme using dna coding and chaos. *Electronics*, *12*(24), 4895. https://doi.org/10.3390/electronics12244895

Lawnik, M., Moysis, L., & Volos, C. (2022). Chaos-based cryptography: Text encryption using image algorithms. *Electronics*, *11*(19), 3156. https://doi.org/10.3390/electronics11193156

Qin, Y., & Zhang, B. (2023). Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal. *Applied Sciences, 13*(14), 8117. https://doi.org/10.3390/app13148117

Shahzad, K., Zia, T., & Qazi, E. U. H. (2022). A review of functional encryption in IoT applications. *Sensors*, *22*(19), 7567.https://doi.org/10.3390/s22197567

Sheng, Y., Li, J., Di, X., Li, X., & Xu, R. (2022). An image encryption algorithm based on complex network scrambling and multi-directional diffusion. *Entropy*, *24*(9), 1247. https://doi.org/10.3390/e24091247

Ulybyshev, D., Rogers, M., Kholodilo, V., & Northern, B. (2023). End-to-end database software security. *Software*, *2*(2), 163-176. https://doi.org/10.3390/software2020007

Wu, X., & Sun, W. (2014). Extended capabilities for XOR-based visual cryptography. *IEEE Transactions on Information Forensics and Security, 9*(10), 1592-1605. https://doi.org/10.3390/engproc2023055065

Wu, J., Zhang, J., Liu, D., & Wang, X. (2023). A multiple-medical-image encryption method based on SHA-256 and DNA Encoding. *Entropy*, *25*(6), 898. https://doi.org/10.3390/e25060898

Wang, Z., Yao, Y., Tong, X., Luo, Q., & Chen, X. (2019). Dynamically reconfigurable encryption and decryption system design for the Internet of Things information security.

Sensors, *19*(1), 143. http://dx.doi.org/10.3390/s19010143

Zhang, X., & Wang, X. (2018). Remote-sensing image encryption algorithm using the advanced encryption standard. *Applied Sciences*, *8*(9), 1540. 1540.https://doi.org/10.3390/app8091540