Image Authentication with Tampering Localization using Chaotic and Neural Mapping

Dattatherya, K. Suresh, M. MadhaviLatha and Manoj Kumar Singh

Abstract— This paper proposes a new approach to authenticate the image using combination of different chaotic maps along with a newly developed a kind of chaotic neural network .They are integrated to develop the authentication code for each pixel available in the image. This authentication code is carried by transmitted image itself near lossless image content quality and need not required any extra memory requirement. Initial parameter sensitivity and aperiodicity of chaotic maps and its integration with other chaotic map and a chaos based neural network are utilized to create the uncertainty in predictability of authentication code in association with image pixels. Developed method is applicable to work for gray as well color images with very little extra requirement in terms of computational complexity. Proposed method is not only authenticated the image but also define the locations of tampering hidden in the image with very high efficiency.

***Keywords*—** Image Authentication, Localization, Chaos, Chaotic map, Neural Network..

I. INTRODUCTION

IN past decade there is rapid developments in computer networks and multimedia transmission (e.g. digital image, audio and video data) in association with the rapid growth of Internet connectivity, this imposes the requirement of secure mechanism for data exchange over the Internet. Transmitting and storing digital data has brought about several security issues. With ease it is possible now to manipulate the digital image and modified image make it available to others. Therefore at present integrity of digital image has become a major issue. Indeed, from their digital nature, multimedia documents can be duplicated, modified, transformed, and diffused very easily. In this context, it is important to develop systems for copyright protection, duplication protection, and authentication of content and identifying the location where tampering has given. Image authentication can be achieved by embedding a message into the image and that embedded message is derived directly from the image itself. When an image is tampered with, then the authentication message derived from the tampered image will be different from the original message.

Chaos theory was discovered by Edward N Lorenz in 1993 [1]. Since 1993, Chaos theory has been applied for many different research areas, such as mathematics, physics, engineering, biology, economics, and philosophy, etc. [2].with time many researchers have observed that there is a close relationship between chaos and cryptography [3-4]. The main difference between chaos theory and cryptography is that cryptosystems work on a finite field, while chaos is meaningful only on a continuum. The authentication schemes can be divided into two categories: digital signature based schemes and digital watermark based schemes. A digital signature can be either an encrypted or a signed hash value of image contents and/or image characteristics. The major drawback of signature based schemes is that they can detect if an image has been modified, but they cannot locate the regions where the image has been modified [5-6]. To solve this problem, many researchers have proposed watermarking based schemes for image authentication [7–10].Various fragile watermarking techniques have been proposed for image authentication and tamper detection. In [11] Sanjay Rawat, Balasubramanian and Raman proposed, a chaos based watermarking scheme for image authentication and tamper detection. In [12] Hongxia Wang and BangxuYin proposed a perceptual hashing-based robust image authentication scheme, which applies the distributed processing strategy for perceptual image hashes and can provide compactness, visual fragility, perceptual robustness, and security in digital image authentication for wireless multimedia sensor network. In [13] Rongrong Ni, QiuqiRuan, Yao Zhao, and Yanxia Wang have proposed an image authentication scheme which is based on a chaotic system with feedback and palm characteristics. To identify the sender of an image and prevent denying event, biometrics information of the sender is applied in authentication solution. A feature vector of palm is extracted and converted to a stream of bits. Where after, the authentication codes and the palm feature bits are encrypted using the public key. A entropy based concept of fragile watermarking technique proposed by

Dattatherya is with Dayananda Sagar College of Engineering, Bangalore - 560078, India; e-mail: datta-tce@dayanandasagar.edu.

K. Suresh is with Dayananda Sagar College of Engineering, Bangalore - 560078, India; e-mail: suresh_int@dayanandasagar.edu.

M. MadhaviLatha is with JNTU College of Engineering, Hyderabad - 500085, India. e-mail: mmadhavilatha@jntu.ac.in.

Manoj Kumar Singh is with Manuro Tech Research, Bangalore-560097, India, e-mail: mksingh@manuroresearch.com.

Young-Long Chen, Her-TerngYau and Guo-Jheng Yang [14] in which image is processed by Arnold's Catmap to become an order less image which is then divided into blocks. A chaotic watermark is obtained with logical operation between the binary watermark and the binary chaotic image. A general framework for fragile watermark is proposed in [15] and a concept presented based on chaotic pattern of image difference defined with actual image to generate the watermark. Dattatherya, S. Venkata Chalam and Manoj Kumar Singh, have presented a unified approach to compress, secure and authenticate the image with the concept of degree of correlation [16]. In [17] Dattatherya, S. Venkata Chalam & Manoj Kumar Singh, have presented A statistical based parametric concept for fast image authentication, which utilized the various moments. In [18] Eric Kee, Micah K. Johnson and Hany Farid have proposed on the signature code available in camera from header of JPEG image authentication method. Bartolini F. Tefas A. Barni M. and Pitas I revealed semi fragile watermarking scheme for video surveillance, which is based on generating watermark sequence using pseudorandom number with threshold [19]. Kostopoulos I, Gilani, S.A.M and Skodras A.N. explained about the concept color image authentication with watermarking scheme, where embedding process applied with a secret key which map the position of pixels[20].

II. Image Authentication System Characteristics

There are various characteristics involved to define the quality of developed authentication system broadly characteristics can be consider as shown in fig1.Authentication system must be sensitive towards malicious manipulations such as cropping or altering the image in specific areas. The system should have capability to locate precisely any malicious alteration made with the image and verify other areas as authentic. The system may need the ability to restore, tampered regions in order to allow the user to know what the original content of the manipulated areas was. This is a difficult task and quality of restoration heavily depends upon locations of tampering and tampered area. Authentication data should be embedded in the image, such as a watermark. Depending on whether authentication data is dependent or not on the image, a full-blind or a semi blind mode of extraction is required. Contrary to classical security services such as copyright protection, an authentication service requires an asymmetrical watermarking (or encryption) algorithm (i.e., only the original hosts can secure it, but other users can get the visual content of an image). Authentication data should not visible under normal visual observation. It is a question of making sure that the visual impact of watermarking is as weak as possible so that the watermarked image remains faithful to the original. It must not be possible for others to forge the authentication data. Protocols under which the authentication defines are an important aspect of any image authentication system; It is obvious that any algorithm or a rule alone cannot assure the guarantee of authentication. It is necessary to define a set of rules and specifications describing the operation and rules of the system, such as the management of the keys or the communication protocols between owner, seller, client, and so forth. In fig1 the important characteristics of image authentication system is shown.

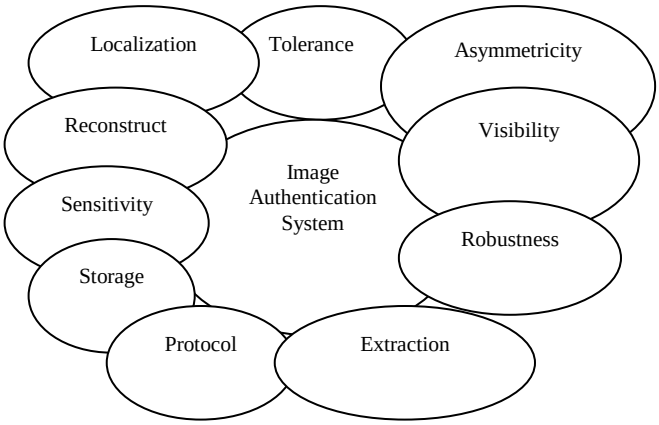


Fig. 1 Image Authentication characteristics

III. CHAOS

Chaos theory refers to mathematical models capable of producing chaotic patterns in successive values of the dependent variables. Chaos models are nonlinear in nature, and can be best outlined by comparing them with linear models. Chaos theory can be considered as the qualitative study of unstable aperiodic behavior in deterministic nonlinear dynamical system. With this definition, number of important information can be drawn about the characteristics of chaos. First that the chaos system is dynamical: means it has time varying nature. Second, the behavior of the system is not periodic and unstable. Third, although chaotic behavior is complex, it can have simple causes through deterministic process. Fourth, because the system is nonlinear; it is sensitive to initial conditions; it means that with different initial condition two logistic sequences generated are statistically uncorrelated. (Nonlinearity means that the output of the system is not proportional to the input and that the system does not conform to the principle of additively, i.e., it may involve synergistic reactions in which the whole is not equal to the sum of its parts). Fifth, because the system is deterministic, chaotic behavior is not random even though its aperiodicity and unpredictability may make it appear to be so. On the other hand, because of the instability, aperiodicity and sensitivity to initial conditions, the behavior of chaotic systems is not predictable even though it is deterministic. A final feature of chaos, although not included in the above definition, is that of iteration or feedback, in which the output of the system is used as the input in the next calculation. Systems may display both chaotic and non-chaotic behavior depending on the control parameters used.

A. *Lozi Map*

Chaos theory is recognized as very useful in many engineering applications. An essential feature of chaotic systems is that small changes in the initial parameters for the data lead to vastly different future behaviors, such as stable fixed points, periodic oscillations, bifurcations, and ergodicity. These behaviors can be analyzed based on Lyapunov exponents and the attractor theory. Details about analysis of chaotic behavior can be found in. This sensitive dependence on initial conditions is generally exhibited by systems containing multiple elements with nonlinear interactions, particularly when the system is forced and dissipative. Sensitive dependence on initial conditions is not only observed in complex systems, but even in the simplest logistic equation. The application of chaotic sequences can be an interesting alternative to provide the search diversity in a search solution procedure. Due to the non-repetition of chaos, it can carry out exploration at higher speeds than probabilistic stochastic ergodic searches .The design of approaches to improve the convergence of chaotic optimization is a challenging issue. A novel chaotic approach is proposed here based on Lozi map .The Lozi's piecewise liner model is a simplification of the He´non map and it admits strange attractors. This chaotic map involves also non-differentiable functions which difficult the modeling of the associate time series. The Lozi map can be define by (1) and (2).

$$S(t+1) = 1 - P.|S(t)| + y(t) \quad (1)$$

$$y(t) = Q.S(t) \quad (2)$$

Where '*t*' is the iteration number. In this work, the values of y are normalized in the range [0,1] to each decision variable in n-dimensional space of optimization problem. This transformation is given by (3)

$$Z(k) = \frac{y(k) - \lambda_{\min}}{\lambda_{\max} - \lambda_{\min}} \quad (3)$$

Where y ϵ [-0.6418, 0.6716] and [λ_{max}, λ_{min}] equals to [0.6418, -0.6716].The parameters used in this work are P=1.7and Q=0.5, these values show the sensitivity with respect to initial condition. We have done experiments for two different setting of initial condition and results of generated chaotic sequences are shown in Fig.2.

Chaotic series are generated for two different setting of parameters which are having very slight change in initial condition to show the variations in generated output. In the Fig.2 Data1 is generated with initial value of parameters S=0.200001, y=0.2 Where as data2 is generated with initial value of parameter S=0.2, y=0.2. Even there is very little difference in initial condition the generated, variation between two chaotic sequences are shown in Fig.2 for 50 samples. With the observation of Fig.2 it is very clear there is a very significant difference between these two chaotic sequences. This will make really a very difficult environment for attacker to guess the parameters of initialization, in result more robust solution.

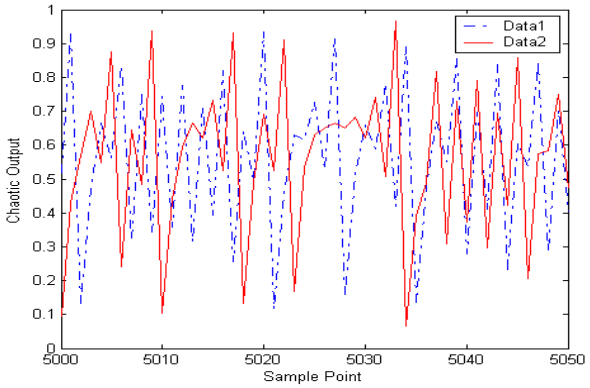


Fig.2 Sensitivity of chaotic sequence with initial condition in Lozi map

B. *Logistic Difference Equation*

Logistic difference can be described as (4)

$$X[t+1] = \lambda * X[t][1 - X[t+1]] \quad (4)$$

This is capable of diverse behavior and depends on the value of λ. If $1<\lambda<3$, the fixed point for the equation is defined as $X=1-\lambda^{-1}$. For $\lambda=3$, system bifurcates to give a cycle of period two which is stable for $3<\lambda<1+6^{0.5}$. As λ increases beyond this value successive bifurcation give rise to a cascade of period doubling which lead to an apparently chaotic sequence for $3.57 < \lambda \leq 4$. For different value of λ=3.9295 and λ=3.7898 and initial condition X(0)=0.2 for both cases, chaotic sequences are generated and results are shown in Fig.3.

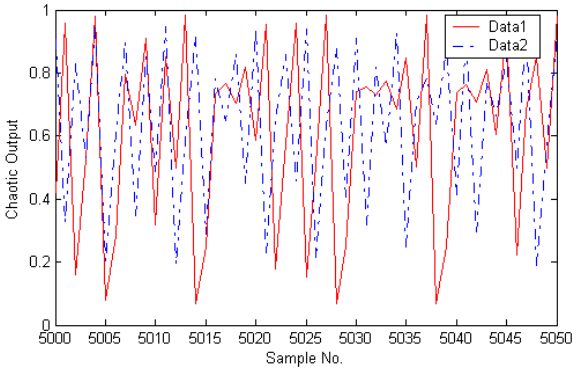


Fig.3 Sensitivity of chaotic sequence with initial condition in Logistic Difference equation

IV. ANN LEARNING WITH CHAOS

The use of heuristic algorithms for optimizing nonlinear functions is an important and growing field of research; this is due to the fact that in mathematics, engineering and sciences, the maximization or minimization of highly nonlinear functions is a common, important and challenging problem. This difficulty is explained by the complexity of the objective function, the restrictions imposed on the problem, the presence of the so-called multiple local minima and the limitations of many optimization methodologies. It is a well-known fact that gradient-based optimization algorithms are trapped within local optimum points. It is possible to think chaos theory can be used in the development of novel techniques for global

optimization. The use of chaotic sequences instead of quasi random number generators seems to be a powerful strategy for improving many traditional heuristic algorithms and their main use is in escape of local minima points.

Chaos based learning method can include two major steps. Firstly, based on the chaotic map define a chaotic sequence generator. Generate a sequence of chaotic points and map it to a sequence of design points in the original design space. Then, calculate the objective functions with respect to the generated design points, and choose the point with the minimum objective function as the current optimum. On the other hand, Neural Networks is one of the most interesting areas of A.I. of which the well-known characteristic is the learning ability. However the training of networks is being argued to improve it. The back-propagation algorithm is very popular gradient descent method for training feed forward neural networks. In its simplest form, it performs fixed step size, steepest descent on an error surface in parameter space. The error surfaces may be highly nonlinear and quite complicated, forcing the use of very small step size to ensure stable convergence of the search procedure. This makes the back propagation algorithm really slow and trapped in suboptimal local minima. Both global optimization and faster convergence are two keys issues of training algorithms. This work proposes an algorithm based on the chaotic sequence generator with the highest ability to adapt and reach the global optima. Proposed learning algorithm formulation has described in Fig. 4 where first global search method explored the region of optimal solution and local search method provides the fine tuning towards optimal solution in the global region. Details of global and local search have described in algorithm as step 2 and step3.

A. Mathematical formulation of learning algorithm

ANN learning algorithm can be treated as finding the optimal value of weights X, which could minimize the error function

$$F(X),\ X=[x_1,x_2,.....x_n]$$

Subjected to $\{x_i\}\in[L,U]$, for $i=1,2,.....n.$

Where F is the objective function, and X is the decision solution vector consisting of n variables $x_i \in R^n$ bounded by lower (L) and upper limits (U).

ANN learning procedure using chaotic map is given as follows:

Inputs definition:

$X=[W_h,W_o]$ Where W_h the hidden layer is weight and W_o is the output layer weight.MG: maximum number of iterations of chaotic Global search;ML: maximum number of iterations of chaotic Local search; λ : step size in chaotic local search

Outputs definition:

X^* : best solution from current run of chaotic search;

f^* : best objective function (minimization problem).

Algorithm:

Step 1: Initialization of variables: Set $X=1$, where k represents the iteration number. Set the initial conditions of chaotic map. Set the initial best objective function

$$f^*=f(X_0)$$

Step 2: Algorithm of chaotic global search:

Begin
While k ≤ MG Do
$X_i(k) = Li + Z_i(k)\,(U_i - L_i),\ i=1,2,\ldots\ldots n$
If $f(X(k)) < f^*$ *Then*
$X^* = X(k)$
$f^* = f(X(k))$
End If
$k=k+1;$
End While
End

Step 3: Algorithm of chaotic local search:

Begin
While k ≤ ML Do
For i= 1 to n
If r < 0.5, *Then*
(Where r ϵ uniformly generated random number in range [0 1])
$X_i(k)= X_i^* + \lambda Z_i(k)|U_i - X_i^*|$
Else
$X_i(k)=X_i^* - \lambda Z_i(k)|X_i^* - L_i|$
End If
End For

If $f(X(k)) < f^*$ *Then*
$X^* = X(k)$
$f^* = f(X(k))$
End If
$k=k+1$
End While
End

During the chaotic local search, the step size λ is an important parameter in convergence behavior of optimization method, which adjusts small ergodic ranges around X^*. The step size λ is employed to control the impact of the current best solution on the generating of a new trial solution. A small λ tends to perform exploitation to refine results by local search, while a large one tends to facilitate a global exploration of search space solution on the generating of a new trial solution. A small λ tends to perform exploitation to refine results by local search, while a large one tends to facilitate a global exploration of search space.

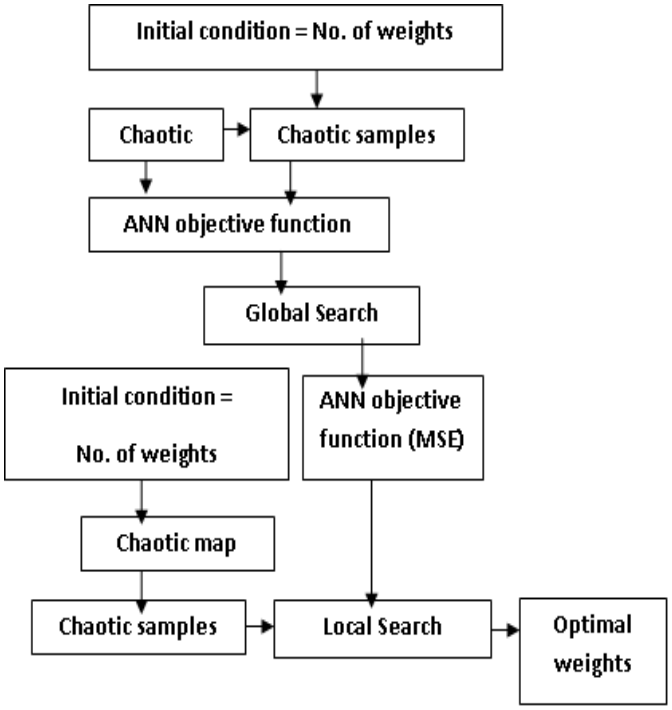


Fig. 4 ANN learning algorithm with chaos.

B. Experimental setup for ANN Learning

A multilayer feed forward architecture having architecture size [1 3 1] is taken with unimodel sigmoid function as transfer function in active node. Self adaptive weight adjustment bias unity input has also applied for hidden layer nodes. Randomly, number of sample pair of points from Lozi chaotic map has selected to define the training data set for neural network. First part of pair is taken as sample inputs for training whereas second part of pair is taken as corresponding target sample point. Random pair selection from chaotic map data not only contains the characteristic of chaos but also include the quality of randomness. This will make neural network more robust in terms of unpredicting its output. Comparison of learning between two different chaos based method namely Lozi map and Logistic difference equation as defined in section have developed .To have comparative benefit with chaos based learning , frequently applied gradient based method has also applied and comparison are analyzed in terms of minimization of error and convergence rate. Comparative performance has shown in Fig.5. From graph it is very clear that Lozi map based chaos-ANN learning outperformed in both cases i.e. it has faster convergence rate and deliver less error. There is another very attractive part with chaos based learning is its computation complexity with very less compare to gradient based method.

TABLE I. DATA GENERATION FOR ANN FROM LOZI MAP

Sample no. pairs		Chaotic value	
		[Input]	[Target]
781	971	0.6273	0.3221
10770	2310	0.7226	0.4516
8684	6187	0.5939	0.7009
12062	14319	0.8541	0.9208
14775	14574	0.5259	0.6079
19323	12667	0.2422	0.5737
14301	19363	0.4189	0.7160
12894	563	0.6309	0.3804
19169	6142	0.2908	0.1340
16543	11270	0.7221	0.7049

Parameters Definition**:**

(a) Lozi Chaotic map=P=1.7; Q=0.5; mn = -0.6418; mx=0.6716; LR=-2.048; UR= 2.047; λ =0.001;

(b) Logistic difference equation: LR=0; UR=1; mn=0.2; mx=0.25; λ is defined with uniform random in range of [3.65, 3.95].

In both cases number of iteration in global and local search have taken 50 respectively. Initial conditions are defined with uniform random selection in [mn, mx] independently for each weight and initial value if weights are taken randomly in the range of [LR, UR].

(c) Gradient method: Initial weights have taken randomly in range of [0 1], learning rate=0.9, momentum constant=0.1and total 100 iterations have applied for weight adjustment to minimize the MSE.

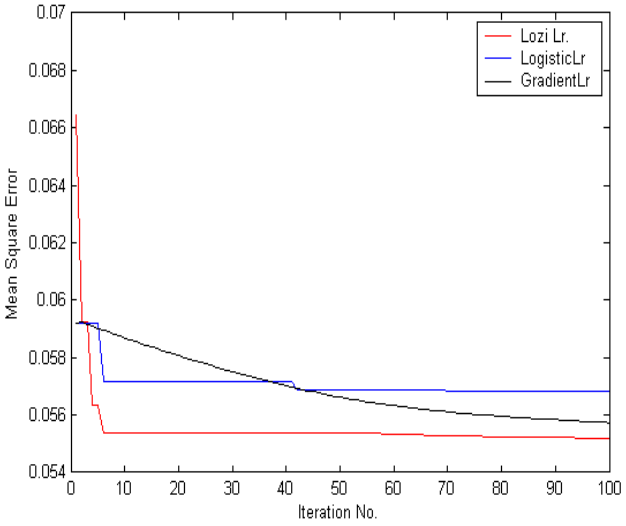


Fig.5 Comparative leaning performance between chaos based learning
and gradient based learning.

V. Proposed Scheme for Image Authentication

The following section explains the proposed authentication scheme.

A. Authentication code generation and embedding in image

1. Generate the random initial condition under define range for Lozi and Logistic map
2. Generate more number of samples as the image have pixels using Lozi map and Logistic map say L_i and D_i
3. Remove the LSB value from all pixels P_{ri} and normalize the pixels, say this is P_i .
4. From taken initial starting sample of Lozi chaotic sequence, start adding samples with normalized pixels i.e $Si = P_i + L_i$
5. Keep the range of S_i within [0,1] by subtracting value more than 1 say Si.
6. From taken initial starting sample of Logistic chaotic sequence, start adding samples with S_{ni}.
   $Z_i = S_{ni} + D_i$
7. Keep the range of Z_i within[0,1] by subtracting value more than 1 say Z_i
8. Take each value of Z_i as an input to the ANN whose weight have trained using Lozi map and generate the corresponding output, say AN_i.
9. Evaluate the mean value of AN_i say this is m. Apply thresholding with $AN_i \geq m$ to generate the authentication code say A_i.
10. With Pr_i add the authentication code A_i to get the image with authentication code.
11. The block diagram of the authentication code generation embedding process is shown in Fig.6.

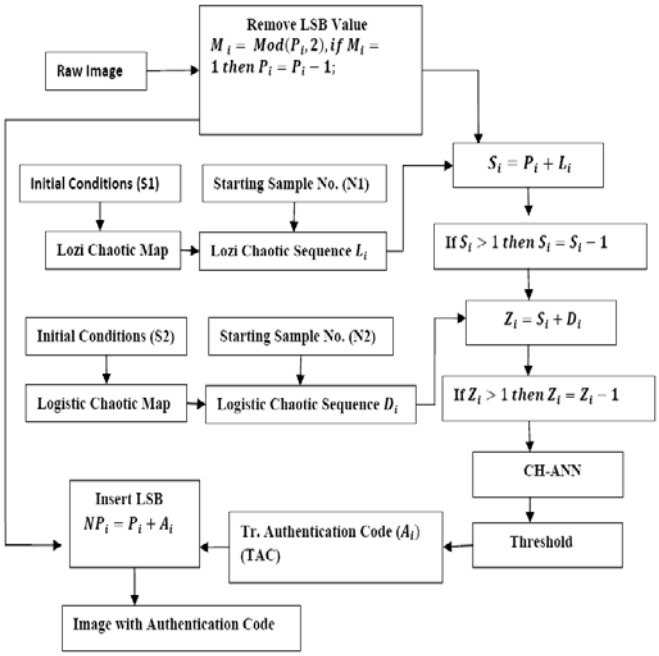


Fig. 6 Authentication code generation and embedding to the image.

B .Authentication code Extraction

Extract the LSB from received image say this A_{ri} and normalized the pixels of image. With defined initial condition chaotic sequences from Lozi and Logistic difference equation have generated. With defined initial starting sample in Lozi sequence, chaotic values are added with pixel and range fixed within [0 1].Chaotic sequence, from defined starting sample of logistic map are added and range is fixed within [0 1].This is a pass to chaotic neural network and generated outputs are threshold with mean value to generate the extracted authentication code with received image say this A_{rei} and comparisons are made with A_{ri} to define the tampering and localization.

VI. Color Image Authentication

Procedure applied for gray image authentication can be extended for color image also. Three color planes in color image separated and in any one color plane, authentication code corresponding to transform gray scale image is embedded with removal of selected plane LSB. Later the entire three planes combine to form the color image with authentication code. The detail flow is given in Fig. 7. For authentication purpose, received color image separated in to different three color plane and embedded code is extracted from one plane. After combining all planes it transform in to gray scale and authentication code extracted and comparisons are made for final decision of tampering.

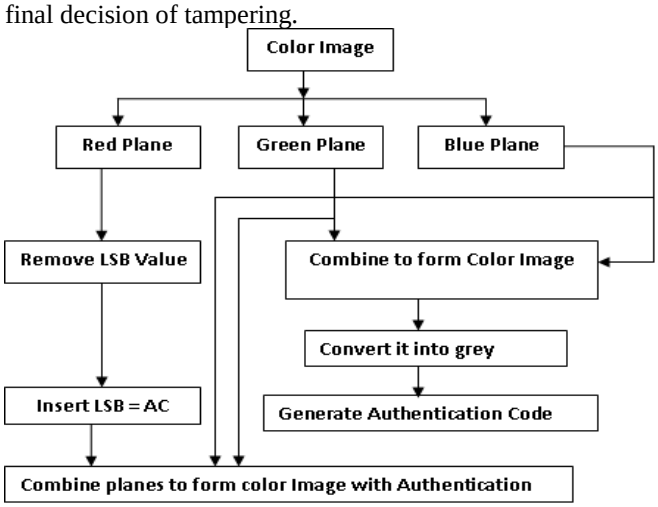


Fig.7 Color image authentication code generation and embedding to image.

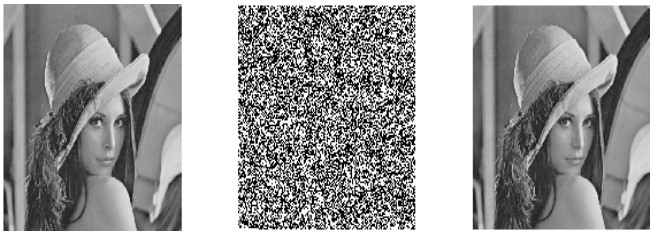
VII. Experimental Results

Various experiments are carried out in this section, to assess the performance of the proposed algorithm. The parameters of Lozi map are taken as P=1.7; Q=0.5; with initial condition defined randomly in range of [0 0.5], whereas for Logistic map it was defined as 0.2 with step size randomly defined in range of [3.58, 3.95].PSNR (Peak Signal-to-Noise Ratio), is used in this paper to analyze the visual quality of the image with authentication code $\tilde{X}$ in comparison with the original image X. For an Image with R rows and C columns, PSNR is defined as follows in (5):

$$PSNR(I) = 10\log_{10}\left(\frac{255^2}{\frac{1}{RC}\sum_{i=1}^{R}\sum_{j=1}^{C}\left(X_{ij} - \tilde{X}_{ij}\right)^2}\right) \quad (5)$$

A. Performance under Content Adding Tampering Attack

In this experiment, 'Lena' image of size 512 × 512 is used. Fig.8 shows the host image, generated authentication code and the corresponding image with Authentication code. The PSNR value of image with authentication code is 51.14dB. Two kinds of content attacks are performed. In first kind of attack is putting the extra bar vertically and in second attack given in terms of small spot over forehead. The tampered image and its detection with position are shown in Fig.10; whereas Fig.9 gives the tampering amplitude in total pixels with each block.



(a) Original Image (b) Authentication Code (c) Image with Authentication Code

Fig .8 Lena Image with and without authentication code.

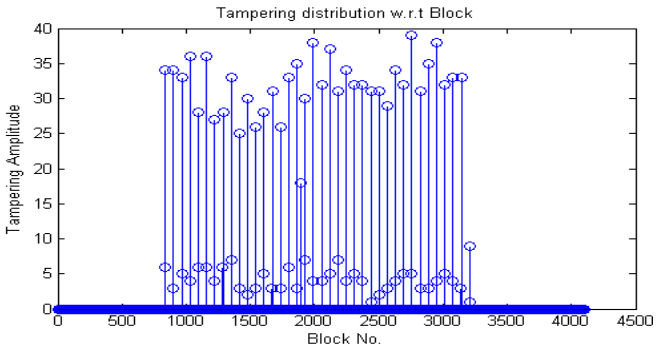
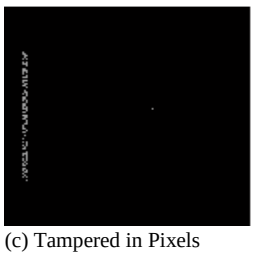


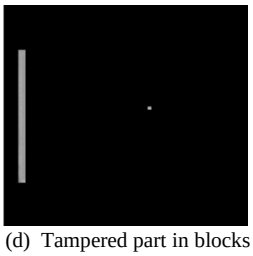
Fig. 9 Tampering detection in block wise

(a) Recevied Image Difference

(b) Authentication Code



(c) Tampered in Pixels

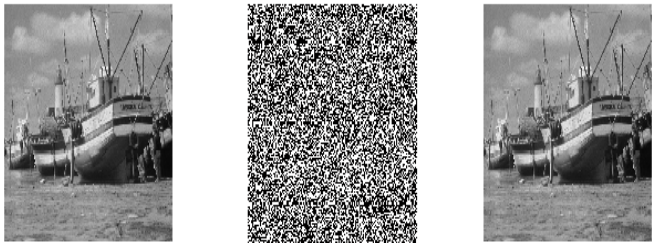


(d) Tampered part in blocks

Fig.10 Received image with tampering and its detection

B. Performance under Content Adding Tampering Attack.

(1) In this experiment, 'Boat' image of size 512 × 512 is used. Fig.11 shows the host image, generated authentication code and the corresponding image with Authentication code. The PSNR value of image with authentication code is 51.13dB. In the tampered image content of written letters in front has changed. Tampering amplitude has shown in Fig.12.The tampered image and its detection with position is shown in Fig13.



a) Original Image (b) Authentication Code (c) Image with Authentication Code

Fig. 11 Boat Image with and without authentication code

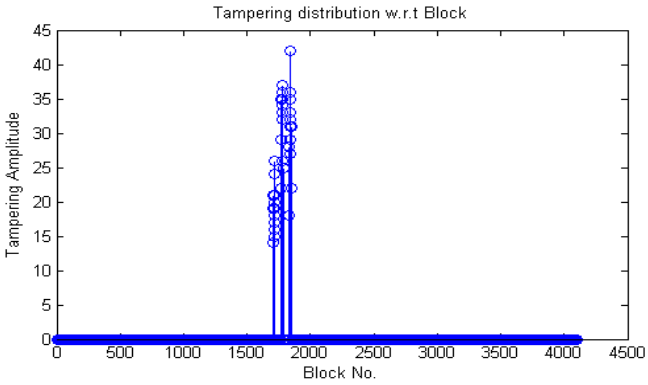


Fig. 12 Tampering detection in block wise.

(a) Recevied Image

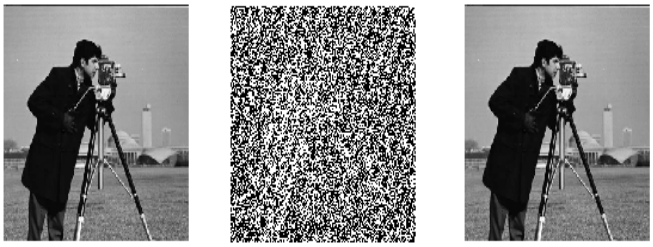
(b) Authentication Code Difference

(c) Tampered in Pixels

(d) Tampered part in blocks

Fig.13 Received boat image with tampering and its detection.

(2) A cameraman image has shown in Fig.14 with the authentication code and has PSNR value 51.14dB. A tower building which is available in original image has removed from the image and authentication results are shown in Fig.15 and in Fig.16.



(a) Original Image (b) Authentication Code (c) Image with Authentication Code

Fig.14 Cameraman Image with and without authentication code.

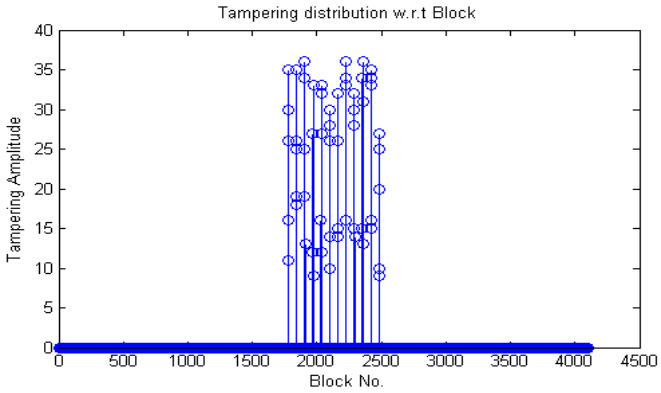
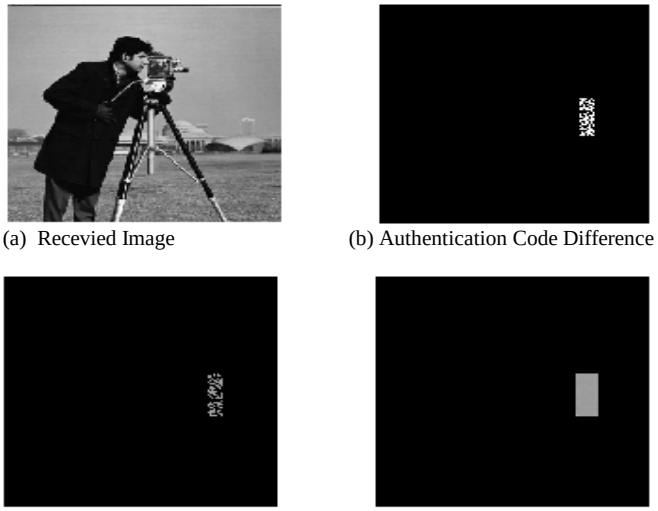


Fig. 15 Tampering detection in block wise

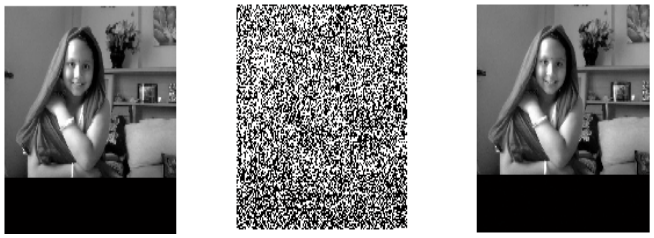


(a) Recevied Image (b) Authentication Code Difference

(c) Tampered in Pixels (d) Tampered part in blocks

Fig. 16 Received Cameraman image with tampering and its detection

(3) Siyasha's image has shown in Fig.17 with authentication code and has PSNR value 51.29 dB. In background there is a picture on wall, which has tampered and defined as a plan frame in tampered image. Results of authentication have shown in Fig.18 and in Fig.19.



(a) Original Image (b) Authentication Code (c) Image with Authentication Code

Fig.17 Siyasha Image with and without authentication code

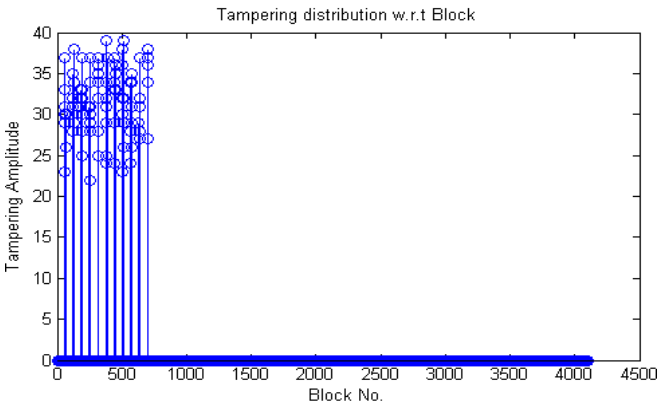
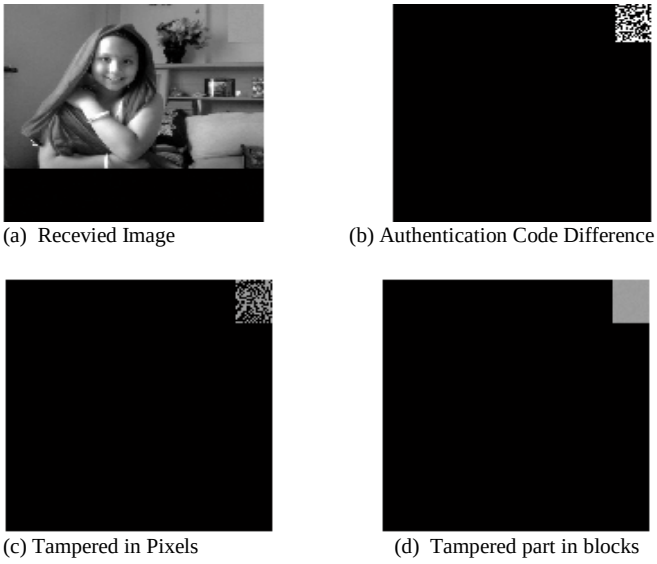


Fig.18 Tampering detection in block wise



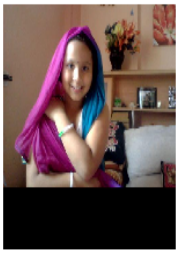
(a) Recevied Image (b) Authentication Code Difference

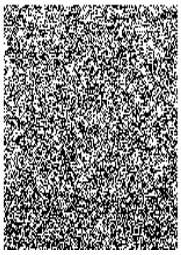
(c) Tampered in Pixels (d) Tampered part in blocks

Fig.19 Received Siyasha image with tampering and its detection

C. Performance under Content Color Tampering Attack

A color image of Siyasha has taken as shown in Fig. 20 with authentication code its PSNR value is 56.04 dB, Color of picture available on has changed without changing the content. Performance of authentication has shown in Fig.20 and in Fig.21.


(a) Original Image


(b) Authentication Code

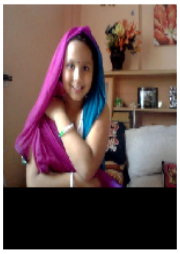
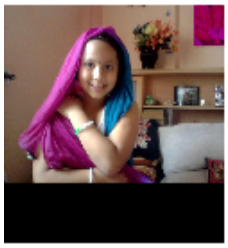

(c) Image with Authentication Code

Fig.20 Siyasha Image with and without authentication code


a) Recevied Image


(b) Authentication Code Difference


c) Tampered in Pixels


(d) Tampered part in blocks

Fig.21 Received Siyasha image with tampering and its detection

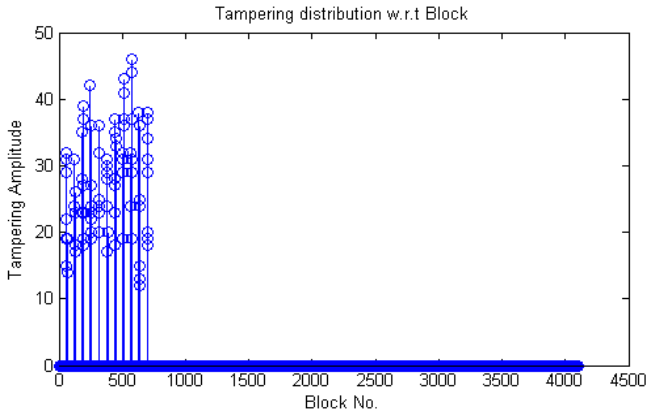


Fig. 20 Tampering detection in block wise

VIII. CONCLUSION

A novel hybrid scheme for image authentication and locating the position of tampered regions is presented in this paper. Combinations of Chaotic maps in association with a new kind of chaotic neural network are used in this scheme to make the scheme highly secure. Since chaotic maps are sensitive to initial values, they are used as keys in our scheme. Extracting the right authentication code is only possible if someone has correct information about the initialization of both chaotic maps and neural network weights. It is impossible to extract this information from image pixels. The proposed schemes completely destroy the relationship available among pixels in generation of authentication code. Experimental results show that this scheme has not only efficient in authentication and localization but also have minimal damage to the original image and it can applicable to gray scale as well as color image too.

ACKNOWLEDGMENT

The research work is completed at Manuro Tech Research; Bangalore, India .Authors expressed their thanks to associated members.

REFERENCES

[1] Lorenz E.N 1993,"The Essence of Chaos-University of Washington Press", Seattle, WA.

[2] B. Hao.1993, "Starting with parabolas: An Introduction to chaotic dynamics", Shanghai China: Shanghai Scientific and Technological Education Publishing House.

[3] Brown, R and Leon, O. "Clarifying chaos: Examples and Counter examples", International Journal of Bifurcation and Chaos, 6(02), pp. 219 - 249, DOI: 10.1142/S0218127496000023, 1996.

[4] Dachselt F and Schwarz. W. "Chaos and Cryptography. Circuits and Systems. Fundamental Theory and Applications", IEEE Transactions, 48(12), pp.1498-1509, DOI- 10.1109/TCSI.2001.972857,2001.

[5] Dittmann J, Steinmetz A and Steinmetz R, "Content-based Digital Signature for Motion Pictures Authentication and Content-fragile Water marking", Proceedings of the IEEE International Conference on Multimedia Computing Systems, pp. 209–213, 1999. DOI:10.1109/MMCS.1999.778274

[6] Lu CS, Liao HYM and Sze C.J., "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme", proceedings of the multimedia security workshop, 8th ACM International Conference on Multimedia, pp.115–118,DOI - 10.1109/TMM.2003.811621, 2003.

[7] Eggers JJ and Girod B., "Blind Watermarking applied to Image Authentication" in Proceedings of IEEE International Conference on Acoustics, Speech and Signal processing.volume-3, pp. 1977–1980, 2001. DOI-10.1109/ICASSP.2001.941335

[8] Kundur D and Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication. In: Proceedings of the IEEE special issue on identification and protection of multimedia information. Vol. 87,pp. 1167–1180, DOI- 10.1109/5.771070,1999.

[9] Lin, E.T., Podilchuk C.I and Delp, E.J., "Detection of image alterations using semi-fragile watermarks", Proceedings of SPIE conference on Security and Watermarking of Multimedia Contents II, pp. 152– 163, http://www.ece.purdue.edu/~ace, or +1 765 494 1740. 2000.

[10] Wang M.S and Chen W.C.,'A majority-voting based Watermarking Scheme for Color Image Tamper Detection and Recovery", Computer Standards & Interfaces, vol.29, pp.561–570, 2007. DOI-10.1016/j.csi.2006.11.009.

[11] Sanjay Rawat and Balasubramanian Raman, "A Chaotic System Based fragile watermarking scheme for Image Tamper Detection" ,Elsevier, Int. J. Electronics. Communication (AEÜ) vol-65 pp.840– 847, year-2011, http://dx.doi.org/10.1016/j.aeue.2011.01.016.

[12] Hongxia Wang and Bangxu Yin , "Perceptual Hashing-Based Robust Image Authentication Scheme for Wireless Multimedia Sensor Networks", International Journal of Distributed Sensor Networks, Vol 2013, , http://dx.doi.org/10.1155/2013/791814.

[13] Rongrong Ni, QiuqiRuan, Yao Zhao, and Yanxia Wang, "Image Authentication based on Chaotic System with Feedback and Palm Characteristics", 6thEuropean Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August, pp. 25-29, www.eurasip.org/Proceedings/Eusipco/Eusipco2008/.../1569103942. 2008.

[14] Young-Long Chen, Her-Terng-Yau and Guo-Jheng Yang ,"A Maximum Entropy-Based Chaotic Time-Variant Fragile Watermarking Scheme for Image Tampering Detection", Entropy, pp.3170-3185, 2013, doi:10.3390/e15083260.

[15] Liu,Yao and Wen, Liu ," An image fragile watermark scheme based on chaotic image pattern and pixel-pairs", Applied Mathematics and Computation 185, pp. 869–882,Elsevier, http://dx.doi.org/10.1016/j.amc.2006.07.036 2007.

[16] Dattatherya, S. Venkata Chalam and Manoj Kumar Singh," Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP" International Journal of Image Processing (IJIP), Volume (6) : Issue (1), pp.13-25, 2012.

[17] Dattatherya, S. Venkata Chalam and Manoj Kumar Singh," A Generalized Image Authentication Based On Statistical Moments of Color Histogram" Int. J. on Recent Trends in Engineering and Technology, Vol. 8, No. 1, pp.40-46, http://searchdl.org/public/journals/2013/IJRTET/8/1/32.pdfJan 2013.

[18] Eric Kee, Micah K. Johnson and Hany Farid, "Digital Image Authentication from JPEG Headers" Information Forensics and Security, IEEE Transactions on (Volume:6 , Issue: 3),pp.1066 – 1075, DOI-10.1109/TIFS.2011.2128309,2011.

[19] Bartolini , Tefas A, Barni, M and Pitas I." Image authentication techniques for surveillance applications "Proceedings of the IEEE (Volume:89 , Issue: 10), pp.1403 – 1418, DOI-10.1109/5.959338, 2001.

[20] Kostopoulos I ,Gilani, S.A.M .and Skodras A.N." Colour image authentication based on a self-embedding technique", Digital Signal Processing,14th International Conference on (Volume:2) ,PP.733 – 736,DOI-10.1109/ICDSP.2002.1028195,2002.