Unified Approach with Neural Network for Authentication, Security and Compression of Image: UNICAP

Dattatherya dattugujjar28@yahoo.com
Asst.Prof., Department of TCE
Dyananda Sagar College of Engineering
Bangalore, 500078, India

S. Venkata Chalam sv_chalam2003@yahoo.com
Professor, Department of ECE
CVR College of Engineering
Hyderabad, 501510, India

Manoj Kumar Singh mksingh@manuroresearch.com
Director
Manuro Tech Research
Bangalore, 560097, India

Abstract

The present demands of scientific and social life forced image processing based applications to have a tremendous growth. This growth at the same time has given number of challenges to researcher to meet the desired objectives of either users or from solution perspectives. Among the various challenges, the most dominating areas are: reduction in required memory space for storage or taken transmission time from one location to other, protection of image contents to maintain the privacy and to facilitate the mechanism to identify the malicious modification if there is any, either in storage or in transmission channel. Even though there are number of methods proposed by various researchers and are existed as solutions, questions are remain open in terms of quality, cost and complexity. In this paper we have proposed the concept based on neural network to achieve the quality of compression, protection and authentication all together using the ability of universal approximation by learning, one way property and one to one mapping characteristics correspondingly. With the proposed methods, not only we can authenticate the image but also positions of malicious activity given in the image can be located with high precision. Proposed methods are very efficient in performance as well as carry the features of simplicity and cost effectiveness.

Keywords: Image Compression, Protection, Authentication, Universal Approximation, One-way Property, One to One Mapping, Neural Network.

1. INTRODUCTION

In the past several years there has been an explosive growth in the use of computer networks, whereby digital information such as text, images and other multimedia files are transmitted frequently via the networks. Digital information that is traveling across the networks can potentially be intercepted by someone other than the intended recipient. Due to this digital information such as medical images, intelligence services etc require confidentiality security service. Currently there are several approaches available for protecting digital images; the traditional method of hiding data is to scramble it so that the true message is unknown. Broadly four different approaches for protecting digital images are: compression, digital watermarking, steganography and cryptography. Basically, compression is a process of encoding data to another form by removing all the redundancy that occurs in the data. This encoding technique will change the data into unreadable form as well as reducing the size of the data file. Due to this characteristic, compression is usually employed when transmitting information over the network.

For text file, retrieving back the data that is the process of decompression can be done successfully without any loss of information. However, this is not the case for digital images because most conventional image compression schemes such as Cosine Transforms, Wavelets, and Fractals inevitably produce image distortion or loss of resolution after decompression. These image distortions may include: blurring; visible tile boundaries, introduced image artifacts, and jagged or blurry motion. Further increase in compression will result in worse distortions and image quality can be unacceptable. In security perspective this is not tolerable because the true message and its integrity are lost. Besides this, there are several issues that need to be concerned. Firstly, compression technique employs pattern library for encoding. This means for any group to compress or decompress the information, they must have the pattern library. This raises the issue of distribution. Providing that only authorized groups have the pattern library, then only it can be said that the secrecy of the information is maintained. Another issue is that almost all compression algorithms do not integrate password or key in the process of compression or decompression, this will reduce the security strength of the system. Digital watermarking or also known as digital fingerprinting is another technique that is used for digital image protection. This technique inserts pattern of bits known as signature into a digital image, audio or video file. The signature identifies the image’s copyright information such as profile information, or an identification number and it is integrated within digital files as noise or random information that already exists in the file, thereby making the detection and removal of the watermark difficult. Even though digital watermarking technique is meant for copyright protection, it can be extended for hiding digital images instead of signature. Steganography employs the same idea as digital watermarking. Classical steganography concerns with ways of embedding a secret message in a cover or host message such as a video, audio recording or computer code. The embedding is typically parameterized by a key; whereby without knowledge of this key it is difficult for any third party to detect or remove the embedded material. Both digital watermarking and steganography techniques do not randomize the information but instead it hides the digital image under a host image. The main drawback of these two techniques is that it requires another image whereby the size of the host image must be big enough to accommodate all the bits values of the protected digital image. Another technique for securing digital data is cryptography. Unlike steganography, cryptography does not hide the message but instead scrambles the message through an encryption process to produce an unreadable cipher text. The cipher text needs to undergo a process called decryption in order to retrieve back the original message. Likewise as in steganography, these two processes are done based on a specific key value. As an alternative technique for multimedia data especially image, it has been suggested by several researchers to use chaos encryption. In most of the system, the encryption algorithm manipulates the pixels of an image instead of manipulating the bits of the image. Chaotic maps and cryptographic algorithms have some similarities namely sensitivity to a change in initial conditions and parameters, random-like behavior and unstable periodic orbits with long periods. The desired diffusion and confusion properties required in a cryptography algorithm are achieved through the repeated processing. On the contrary, iterations of a chaotic map spread the initial region over the entire phase space. An important limitation of cryptography is that encryption transformations are defined on finite sets.

2. RELATED WORK

In article [1], authors proposed an extension to the block-based image encryption algorithm (BBIE) scheme that works in combination with Blowfish encryption algorithm. Whereas BBIE is meant for 256-color bitmap images, the proposed technique also handles RGB color images and, for the cases studied, improves the security of digital images. In this technique, enhanced block based image encryption technique (EBBIE) the digital image is decomposed into blocks, then two consecutive operations - rotating each 3D true color image block by 90 degree followed by flipping row-wise down - are performed to complicated the relationship between original and processed image. These rendered blocks are then scrambled to form a transformed confused image followed by Blowfish cryptosystem that finally encrypts the image with secret key. [2] Presented a method of chaotic image encryption called the “Triple-Key” method. In this method, it is required to enter an 80-bit session key in addition to the initial parameter key and the control parameter key. Each of the keys forms just one part of the lock that needs to be opened to obtain the original image. The position of bits in the 80-bit key determines the scrambling of individual pixels in the encrypted image. Low correlation coefficient between adjacent pixels in the encrypted image has achieved, which implies higher security and lower probability of security breach through brute force attacks or statistical analysis. Authors in the paper [3] propose a novel image encryption method based on changing the pixel positions as well as pixel values to confuse the relationship between the cipher image and the plain-image. From the results, it is observed that the proposed technique significantly reduces the correlation among the pixels by shuffling the image matrix using a random vector. Moreover, the scheme has less computational complexity, good security and satisfies the property of confusion and diffusion. Transforming method of original image into the encrypted one using randomly generated vectors has presented in[4]. The original image is decrypted by applying least square approximation techniques on the encrypted image and the randomly generated vectors. In the [5] encryption scheme is proposed based on permutation of the pixels of the image and replacement of the pixel values. The permutation is done by scan patterns generated by the SCAN methodology. The pixel values are replaced using a progressive cellular automata (CA) substitution. The proposed image encryption method satisfies the properties of confusion and diffusion due to the CA substitution. Liao's chaotic neural system, cat map and general cat map are introduced and analyzed respectively in [6].Then, a image encryption scheme by employing the Liao's chaotic system to generate parameters of general cat map is designed. In [7] security of image encryption based on two dimensional chaotic maps has presented. Chaotic maps are often used in encrypting images. However, the encryption has periodicity, no diffusion, and at the same time, the real keys space of encryption is fewer than the theoretical keys space, which consequently results in potential security problems. They have given several ways to solve the problems including adding diffusion mechanism, changing the design of keys and developing a composite encryption system. Authors in [8] presented the concept use of Polynomial Chaotic Maps (PCMs) to provide the security of image. Chaotic maps have good properties such as ergodicity, sensitivity to initial conditions and control parameters, etc. Due to these features, they are good candidate for information encryption. In [9] machine learning based concept has applied by authors for image security. One of the areas of new applications is to design cryptographic systems by using chaotic neural network due to the fact that chaotic systems have several appealing features for information security applications. Encryption algorithm is proposed in [10], which encrypts the plaintext based on alternant of the stream cipher and block cipher. A pseudo-random number is used to control which encryption mode is chosen. Using this algorithm, multiple kinds of files (such as TXT, DOC, WMA, and JPEG) are encrypted and decrypted, and the security of the proposed cryptosystem is analyzed. In [11] a camera signature is extracted from a JPEG image consisting of information about quantization tables, Huffman codes, thumbnails, and exchangeable image file format (EXIF). They have shown that this signature is highly distinct across 1.3 million images spanning 773 different cameras and cell phones. Specifically, 62% of images have a signature that is unique to a single camera, 80% of images have a signature that is shared by three or fewer cameras, and 99% of images have a signature that is unique to a single manufacturer. The signature of Adobe Photoshop is also shown to be unique relative to all 773 cameras. These signatures are simple to extract and offer an efficient method to establish the authenticity of a digital image. Paper [12] proposed an algorithm for image authentication and verification. The algorithm is based on public key. The owner of image extracts the information as watermark information from the image which he wants to transmit to others. The owner embeds the watermark information into the image with public key. Anyone can judge the valid of the watermarked image, and locate the place which has been tampered. In [13] the proposed scheme dynamically generates the watermark using messy models. And, it is embedded inside the image by expanding intra plane difference between any two color planes of images. It is known as intra-plane difference expanding. The proposed scheme is very sensitive to the jittering, geometrical and various filtering attacks. A scheme for JPEG grey scale images is proposed based on a data embedding method that utilizes a secret key and a secret mapping vector in the frequency domain has given on [14]. An encrypted feature vector extracted from the frequency domain is embedded redundantly and invisibly in the marked image. On the receiver side, the feature vector from the received image is derived again and compared against the extracted watermark to verify the integrity and authenticity.[15] has given a semi-fragile watermarking scheme for color image authentication is proposed based on spatiotemporal chaos and SVD (singular value decomposition). Wavelet transform is applied to watermarking. In contrast to conventional approaches where the watermark is embedded directly on the wavelet coefficients, we embed the watermark onto the SVs (singular values) of the blocks within wavelet sub- band. In order to enhance the security, spatiotemporal chaos is employed to select the embedding positions for each watermark bit as well as for watermark encryption. In [16] this paper proposes an image authentication scheme which detects illegal modifications for image vector quantization (VQ). In the proposed scheme, the index table is divided into non-overlapping index blocks. The authentication data is generated by using the pseudo random sequence. Proposed scheme can adaptively determine both the size of the authentication data and the number of the indices in each index block. Then the selected indices are used to embed the secret data to generate the embedded image.

3. PROPOSED SOLUTION

To capture the quality of compression which also has the protection of itself and a mechanism to define the malicious activity involved with the transmitted or stored image is a difficult task. Even though solution are available for each purpose but problem and limitations are appear at various level of performances like quality, speed etc. along with implementation cost and complexity.

To overcome the issues with existing methods and to improve the performance with respect to three most important requirement compression, security and authentication, when image especially transfer through internet ,rather than applying conventional methods ,intelligent method based on artificial neural network taken as solution platform. There are number of qualities available in ANN which can apply for image processing among them universal approximation, one to one mapping and one-way properties selected to achieve the objectives as shown in Figure1.description of these properties given below.

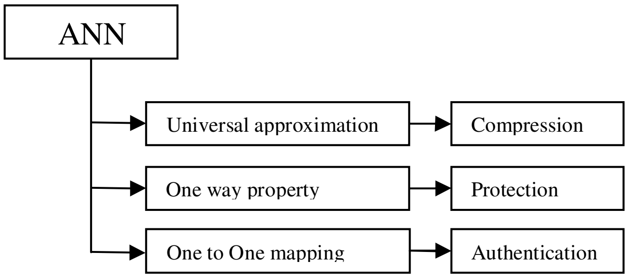


FIGURE 1: ANN properties and its proposed application

(a)Universal approximation

Let F be any Borel measurable or continuous function from $k\subset \Re^n$ on $(0, 1)^m$ and let Φ be any strictly increasing continuous squashing function. Then, for any $\varepsilon > 0$ there exists a multilayer feed forward network N with the quashing function in the output layer and with only one hidden layer such that

$|| N(x)-F(x)|| < \varepsilon , \quad \forall x\in K$ ----------------- (1)

(b) One to one mapping

If there are interaction of two parameters happen under such environment and circumstances so that resultant outcome could be a unique value, then this unique value can be defined as the one to one mapping between these parameters. Mathematically this can be stated as:

$\varphi(x_{i,}\ y)\neq \varphi(x_{j,}\ y)\ ;\ \forall\ j \text{ if } j \neq i\ ;$ ---------------- (2)

Where x_i is external stimulus and having an establish relationship with environment φ contains parameter y and x_j is a new test input in the same environment. This principle is also valid if stimulus is same for different parameter available in environment and this can express as

$$\varphi(x, y_i) \neq \varphi(x, y_j)\ ;\ \forall\ j \text{ if } j \neq i\ ; \qquad \text{----------------} \quad (3)$$

This mapping characteristic can be utilized for authentication and recognition purpose in various applications especially in the field of image recognition where authentication and recognition process cascaded with automatic action as response of recognition.

(C)One-way Property

As it appears by the name a system contains one-way property allow to compute the output from the input easily while very difficult to compute the input from the output. There are two very clear reasons why neural network having one way property
(a) Number of neurons having nonlinear characteristics are involved and interconnected to produce the output.
(b) After learning all previous changes in iterations have lost permanently i.e. no trace available how it has been up to output. Situation will become worse if weights are not available in fact it is impossible to find the input if weights are not available.

Taking a simple neuron model for example, the input P is composed of n elements [p_1, p_2 , p_3 ,…… p_n] while the output is a unique element C. It is defined as:

$$C = f\left(\sum\nolimits_{j=1}^{n} w_j p_j \ +b \right) \qquad \text{-------------------} \ (4)$$

As can be seen, it is easy to compute C from P[p_1, p_2 , p_3 ,…… p_n], while difficult to compute P from C. The difficulty is equal to solve a singular equation. Thus, it is a one-way process from the input P to the output C.

4. IMPLEMENTATION DESCRIPTION

4.1 Preprocessing of Image

Preprocessing is a step which makes the raw data suitable for proper processing. Without which either it is not possible to complete the processing or it may happen with error. From neural network perspectives two different stages required for preprocessing (a) spatial block formation (b) normalization. In spatial block formation image is divided into number of block, each block have a size of m*n pixels, generally m = n. Depends upon the number of pixels in each block input layer neuron number decided. As a rule of thumb about size of block is it should not suppose to too large otherwise it will carry more information which will make difficult to extract local information or should not suppose to be too small otherwise block will not carry proper information about its neighbors. Any moderate size will give a better chance to capture the correlation of pixels in a small local region. Normalization will transfer the pixels value in the range of [0 1] so that it can directly taken as an input for neural network.

4.2 Universal Approximation as a Compression Mechanism

Purpose of compression is to reduce the memory requirement to represent the same image. Fundamentally this is achieved by redundancy available in image. Problem with this quality is redundancy varies from one image to another and in result with same process different compression ratio appears. There are number of application where we required fixed compression ration irrespective of quality of images. To achieve this a feed forward architecture can be taken as solution where hidden layer neuron number are less compare to input layer .For this structure compression ratio directly appear as ratio of number of selected neurons in input layer and hidden layer. Output layer neuron number is same as input layer. With respect to an image for each block training has given to get the learning of correlation available in each block in other word neural network get the approximation knowledge of relationship available in each block. Because there is a large data set available for learning in result after completion of training neural network having capability to define the approximate characteristics available in any type of test image on block basis. Design of compression mechanism has shown in

Figure3-Figure5.Trained output layer weights of neural network called here decompression key which can be passed to receiver only once physically or through secret channel.

4.3 One-way Properties for Security of Compressed Image

As it was stated earlier neural network having characteristics of one-way property. After learning compressed data for each block taken from hidden layer neurons are completely secure. Even though compressed data in channel are integer number but inside the neural network it is transform in to real number which increase level of security further .not only that until the proper weights for decompression are not available it is impossible to decompressed the compressed information. This gives one extra step of security where there are less number of user in group and situation forced them not to revel the others information for example in the case of intelligence services. Even all users are using the same concept of solution but each one will communicate the image with other one only with a proper set of weights which are not available for others.

4.4 One to One Mapping Property for Authentication

Purpose of learning in neural network is to map the input information corresponding to desired output. This property applied here to give the authentication of image with very high precision. With respect to compressed data set one architecture of feed forward network having input layer neuron equal to hidden layer neurons in the compression system and $\lfloor 30\% \rfloor$ of that taken as hidden layer neuron with single neuron in output layer is created. To make the authentication sensitive target of learning given as 0.5.once learning completed for each compressed block generated output is taken as authentication code for that block. Trained weights are taken as authentication key for that particular image and its size is very small even decrease further with higher compression ratio. This authentication key passed to receiver through the secret channel where as authentication code passed through public channel. Detail working process of develop system is shown in Figure2 and algorithmic construction has shown below

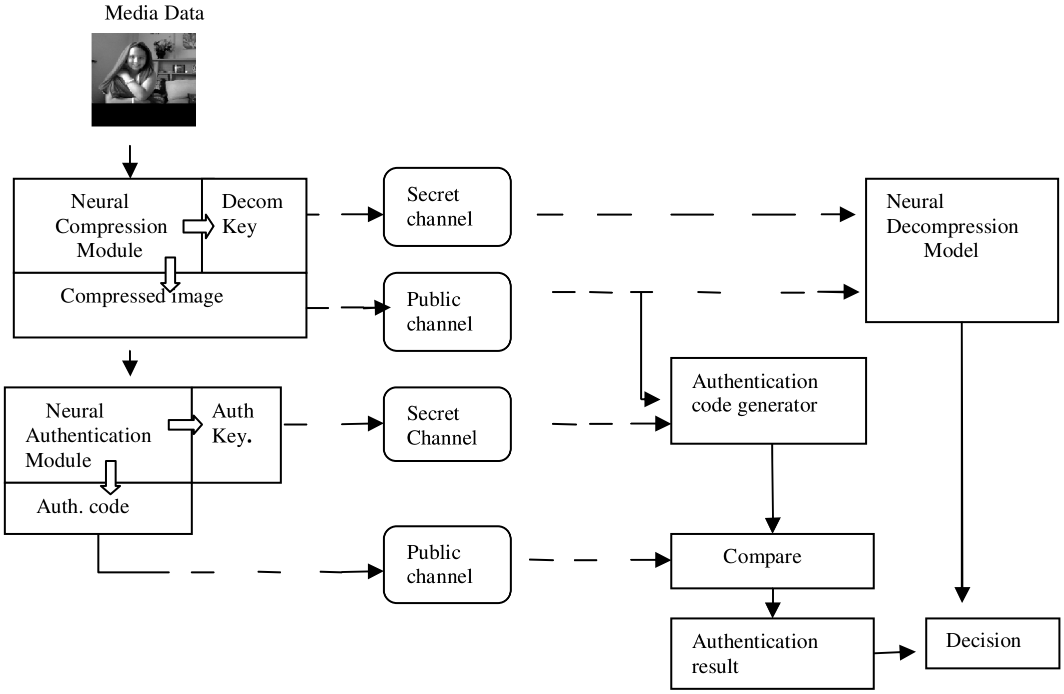


FIGURE 2: Architecture of the proposed multimedia content UNICAP scheme.

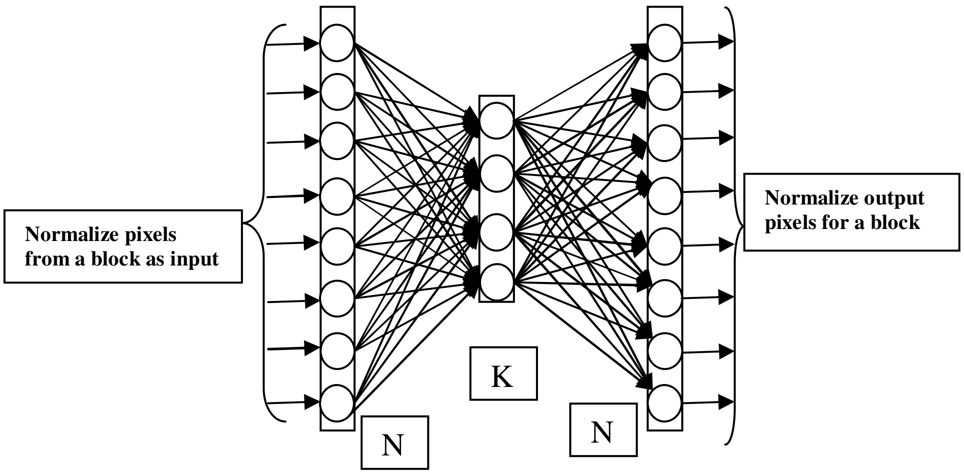


FIGURE 3: Compression architecture of ANN in learning

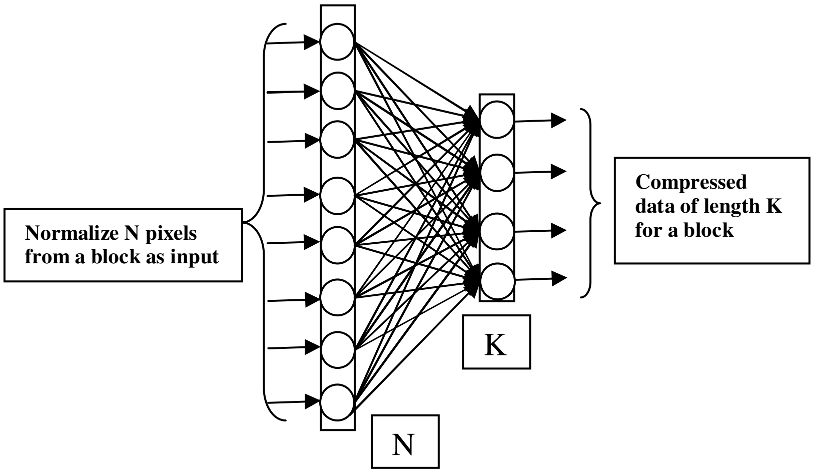


FIGURE 4: Architecture for the compression module

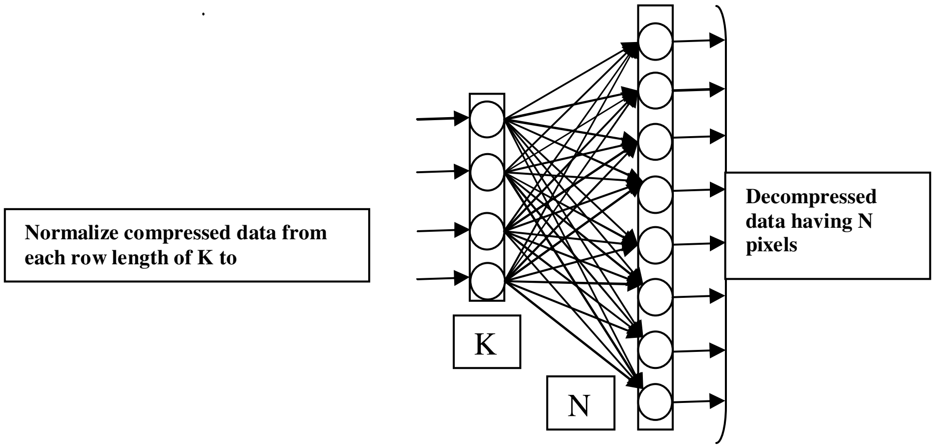


FIGURE 5: Architecture for Decompression module

5. EXPERIMENTS & RESULTS

To get the output with proposed solution for training purpose a gray scale image having size of 'Lena' having 512*512 pixels has taken. Size of block has defined as 8*8 pixels and in result there are 4096 blocks are available. A fully interconnected multi layer feed forward architecture having size [64 64/CR 64] has taken (CR represents compression ratio taken at present 4:1).Bias has also applied for hidden and output layer neuron. Transfer function in hidden and output neurons has taken as unimodel sigmoid function. Back propagation learning algorithm has applied for learning with learning rate equal to 0.1 and momentum rate equal to 0.5 for 500 iterations. Initialization of weights taken as random number derived from uniform distribution in the range of [-1 1].authentication architecture also taken as feed forward architecture and back propagation learning applied for 50 iterations. Performance generated in the experiments for various test images have shown below.

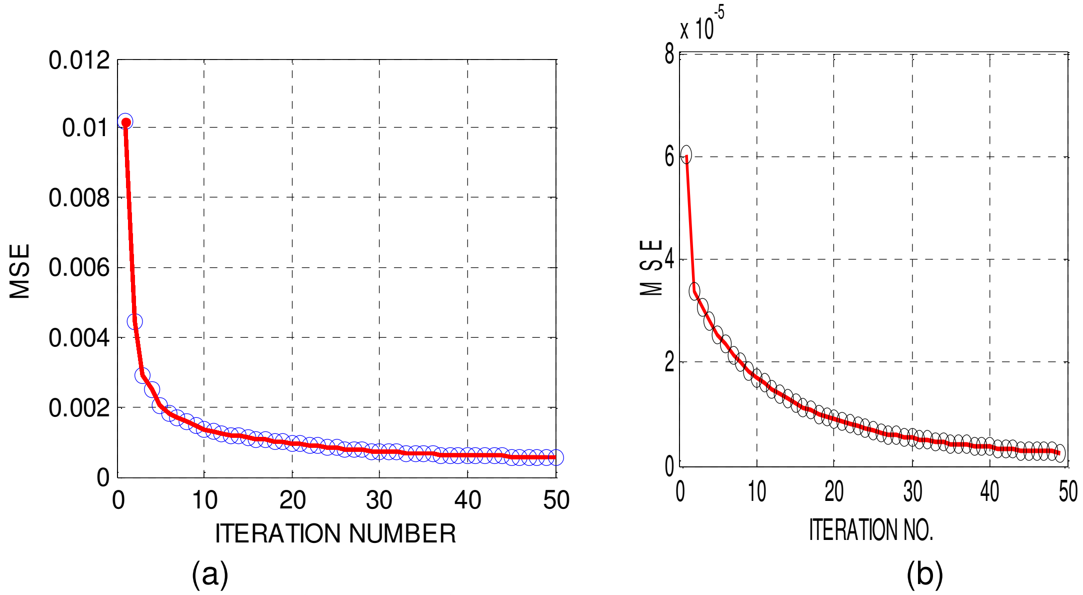
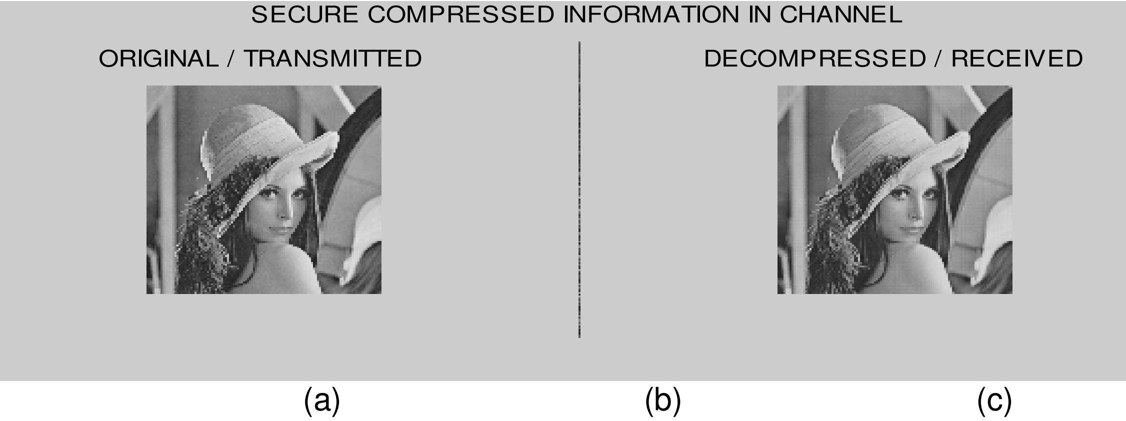
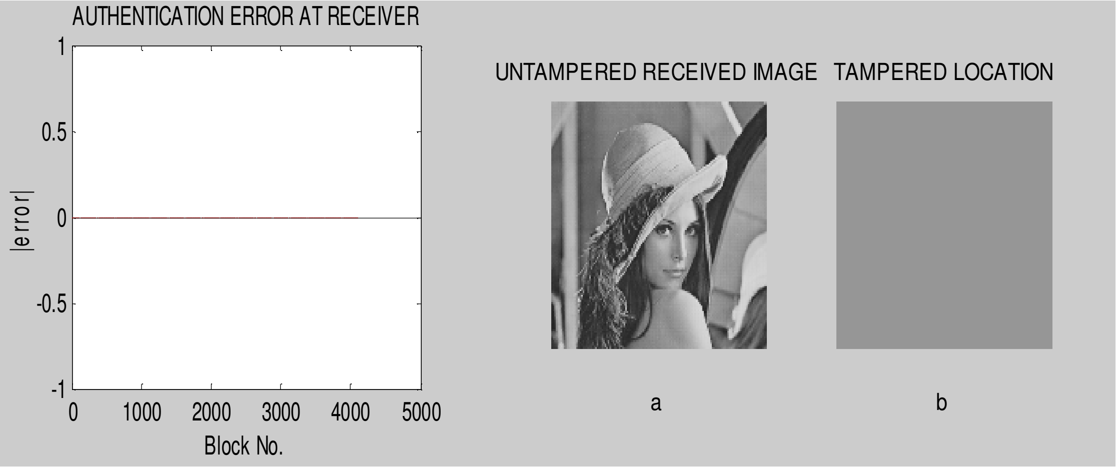


FIGURE 6: UNICAP performance with training image

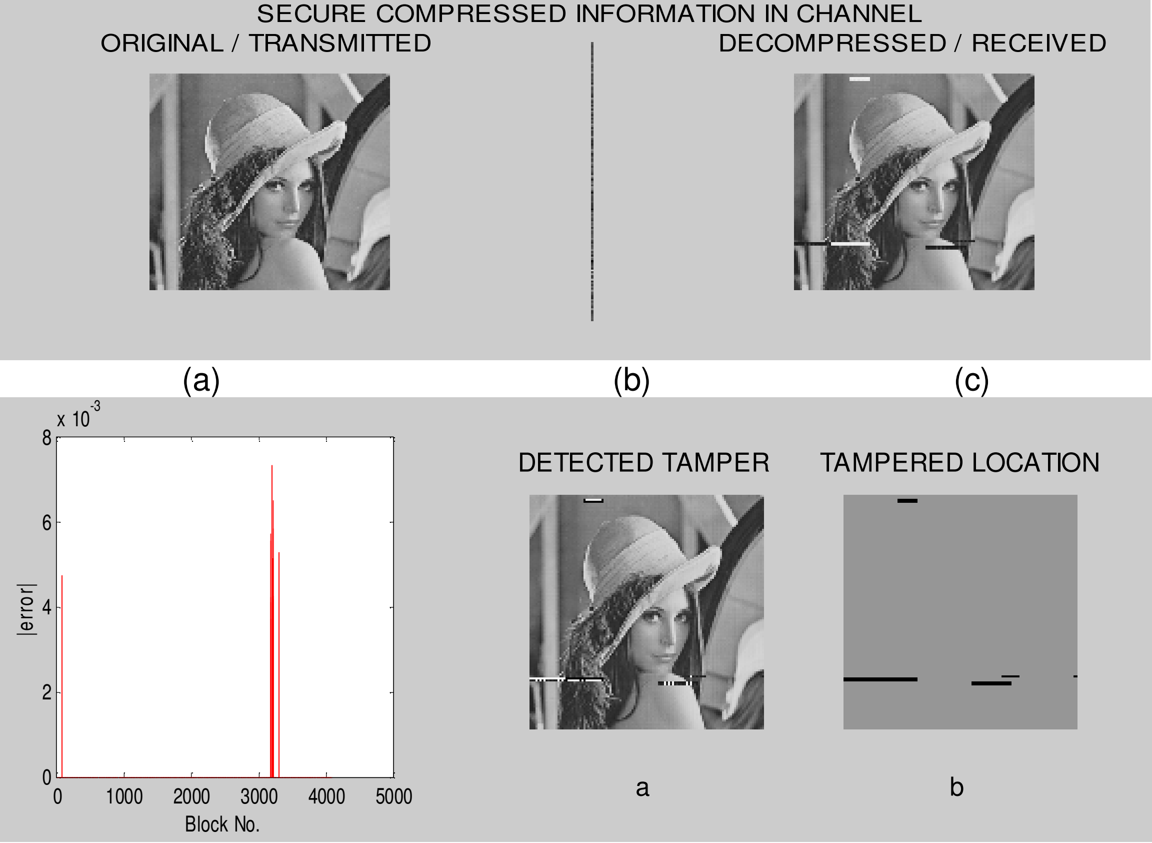




(d) (e) (f)

FIGURE 7: UNICAP performance with training image

Tampered case 1:



(d) (e) (f)

FIGURE 8: UNICAP performance with trained image (bmp format) [a: f]

Tampered case 2:

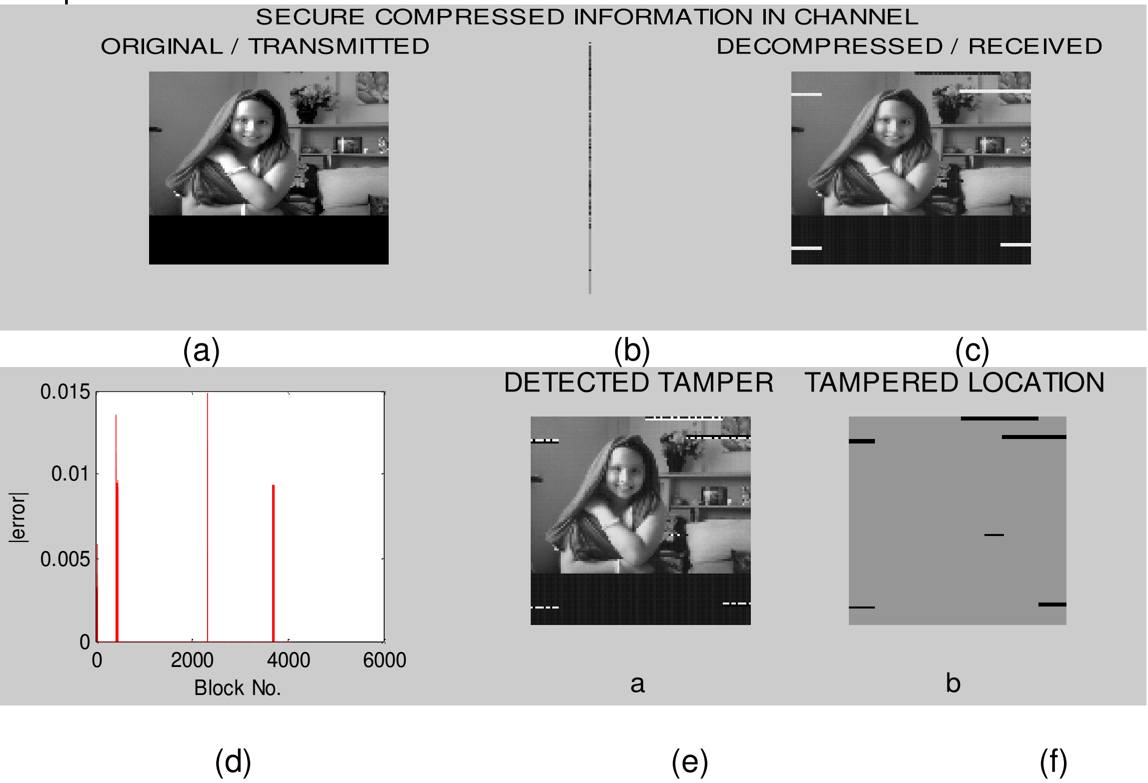


FIGURE 9: UNICAP performance with Test image (jpg format) [a: f]

Tampered case 3:

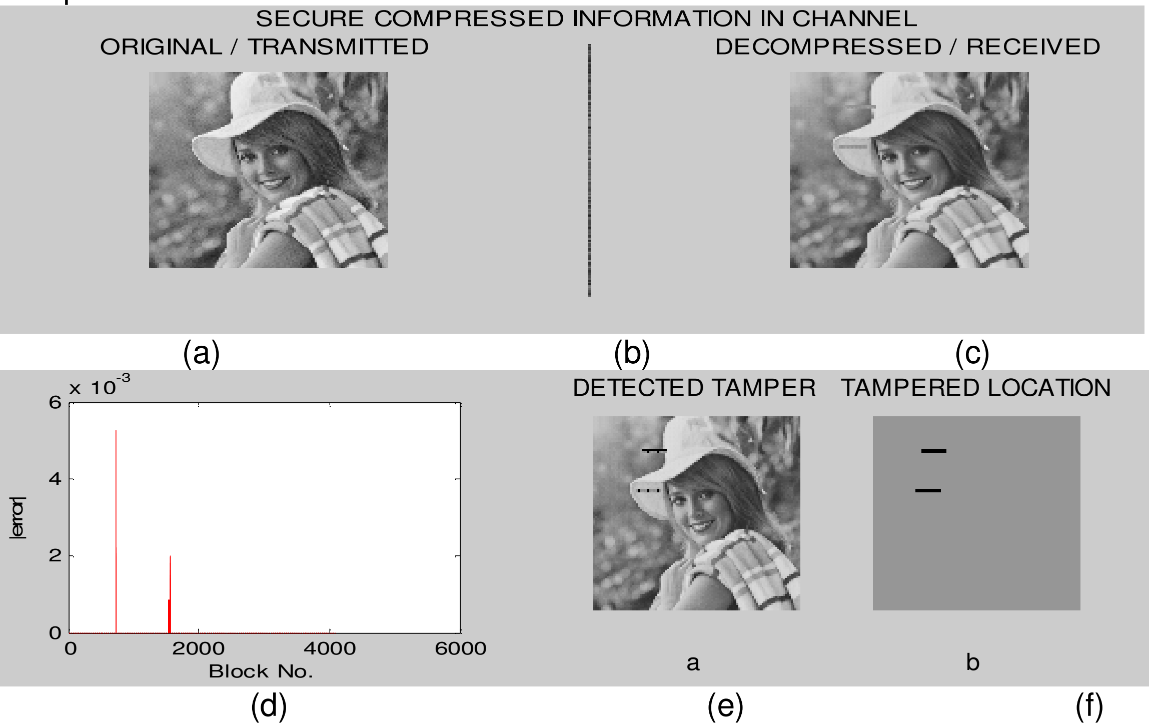


FIGURE 10: UNICAP performance with Test image (Tiff format) [a:f]

Tampered case 4**:**

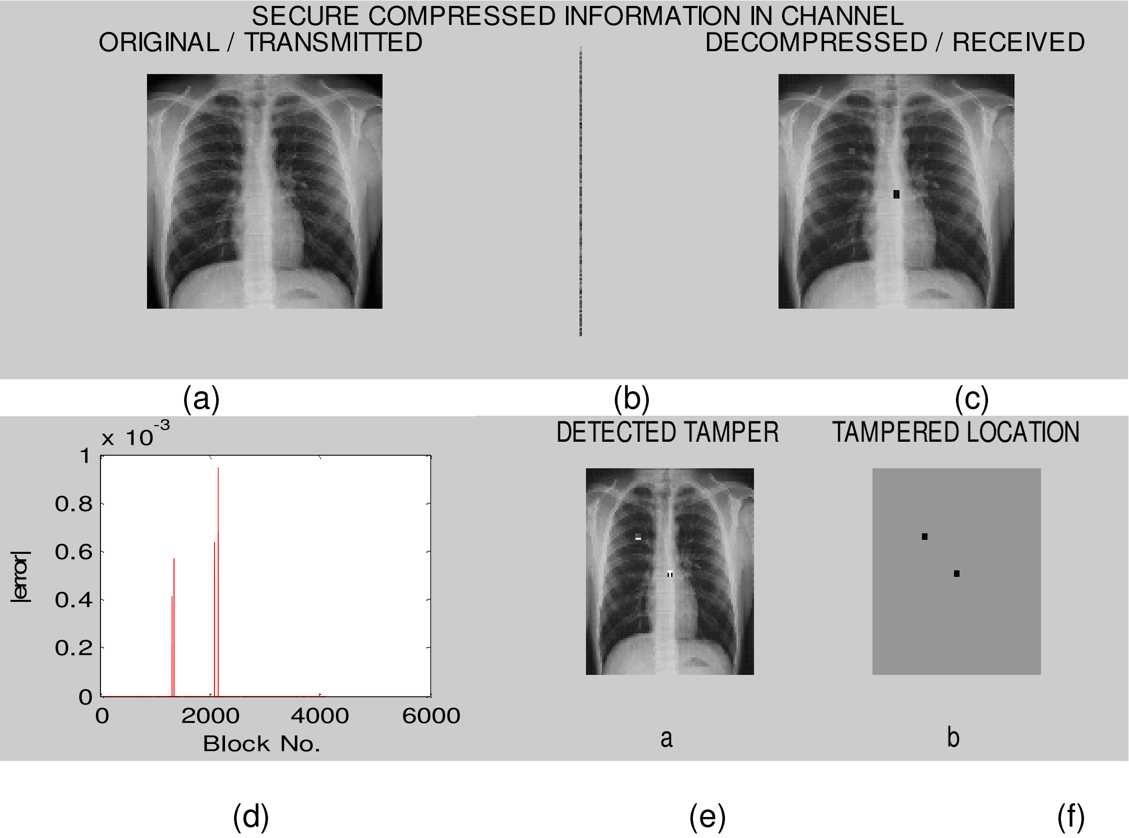


FIGURE 11: UNICAP performance with Test image (bmp format) [a:f]

Performance for various images in different format with various tempered condition have shown in Figure.6 to Figure.11.Learning performance for compression and for authentication code generation have shown in Fig.6 (a) &(b).It is clear from curve that in both case proper learning happen with less number of operations. Performances for different images have shown in Figure7 to Figure11 in subsection of (a) to (f).Definition of information in each subsection has given below:
(a): Original image which has to be transfer from one location to other.
(b): Compressed data display of original image with compression ratio equal to 4.it is appear always as a vertical line hence it does not revel any information and protection available for original image.
(c): Received image after decompression of compressed data, obtained PSNR for each image without tampering is 32.50, 25.6, and 31 correspondingly.
(d): Absolute error in authentication code for each block, higher value indicate level of tampering is high, low value indicate low level tampering where as zero value represents unaltered.
(e): Image with identified tamper location available to clearly see the affect of tampering. Intentionally each block border of tampering made black or white to visualize clearly.
(f): Clearly indicate the position and location of tampering so that user can take the right decision with respect of tampered image.

7. ADVANTAGES OF PROPOSED UNICAP METHOD

(i) A good compression quality can achieve with simple process. Compression ratio is remain same irrespective of quality of image i.e not depends upon redundancy available in the image. This supports the requirement where fixed bandwidth has given for applications.

(ii) With a single image in training data set it is possible to define the compression for any other image having any format and of any quality.

(iii) Very easy means available to change the compression ratio. Solution for different compression ratio can be achieve by just changing the number of hidden layer neurons in architecture and apply the learning.

(iv) Very high Security of compressed data automatically appears without involving any further method exclusively. Level of security is so high it is nearly impossible to extract the information from compressed data.

(v) There is possibility to assign a unique compression facility for each member in a small group.

(vi) Very effectively and precisely authentication of image as well as position of alteration can defined, so that receiver could take the decision of acceptance or rejection of received image with quantity and quality of alteration.

(vii) Simple approach and easy implementation makes the solution cost effective.

8. CONCLUSION

In this paper solution of available fundamental challenges in image based applications at present to providing the protection of image data from unauthorized viewer and how to identify any mischievous alteration given in image has presented. Solution has derived by various integral properties like universal approximation, one-way property and one to one mapping associated with neural network. Direct compression method applied to obtain the fixed compression ratio as well as for protection. It has shown that even with a single image, learning of neural network can have generalized compression capability and decompression is nearly impossible without having optimal weights. For authentication purpose a feed forward architecture with compression data taken as input and single output neuron to generate the authentication code has taken. Proposed method is also securing the position of modification in image. Simplicity and efficiency available in proposed solution make it applicable for practical applications not only for internet based application but also for single system/device based applications.

9. REFERENCES

[1] Syed Ali Naqi Gilani , M. Ajmal Bangash ," Enhanced Block Based Color Image Encryption Technique with Confusion". IEEE ,INMIC 2008. pp. 200 – 206.

[2] Srividya.G, Nandakumar.P "A Triple-Key Chaotic Image Encryption Method". International Conference on Communications and Signal Processing (ICCSP), Feb.2011, pp. 266 – 270.

[3] Nidhi S Kulkarni, Indra Gupta and Shailendra N Kulkarni,"A Robust Image Encryption Technique Based on Random Vector " First International Conference on Emerging Trends in Engineering and Technology", ICETET, July 2008, pp. 15 – 19.

[4] Mahmood Al-khassaweneh and Selin Aviyente, "Image Encryption Scheme Based on Using Least square Approximation Techniques ", IEEE International Conference , May 2008 ,pp. 108 – 111.

[5] Rong-Jian Chen, Wen-Kai Lu and Jui-Lin Lai "Image Encryption Using Progressive Cellular Automata Substitution and SCAN". IEEE International Symposium on Circuits and Systems, ISCAS , Vol. 2, 2005. pp. 1690 - 1693

[6] Shaojiang Deng, Linhua Zhang and Di Xiao,"Image Encryption Scheme Based on Chaotic Neural System "Springer,LNCS, Volume 3497/2005, pp. 810.

[7] Feng Huang and Yong Feng, "Security analysis of image encryption based on two-dimensional chaotic maps and improved algorithm ",Springer, Frontiers of Electrical and Electronic Engineering in China Volume 4, Number 1, 2009, pp.5-9.

[8] Amir Akhavan, Hadi Mahmodi and Afshin Akhshani,"A New Image Encryption Algorithm based on One-Dimensional Polynomial Chaotic Maps",springer,LNCS, 2006, Volume 4263, pp.963-971.

[9] Jun Peng and Du Zhang,"Image Encryption and Chaotic Cellular Neural Network", Springer 2009.pp. 183-213,

[10]. Xingyuan Wang, Xiaojuan Wang, Jianfeng Zhao and Zhenfeng Zhang,"Chaotic encryption algorithm based on alternant of stream cipher and block cipher", Nonlinear Dynamics, Volume 63, Number 4, Springer 2011, pp.587-597.

[11] Eric Kee, Micah K. Johnson, and Hany Farid, "Digital Image Authentication From JPEG Headers", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 6, n. 3, Septmber 2011, pp. 1066 – 1075.

[12] Li Lizong; Gao Tiegang, Gu Qiaolun. Bi Lei. "An image authentication and verification based on public Key ",International Conference on Artificial Intelligence and Computational Intelligence Nov. 2009 , pp. 389 – 392.

[13] Poonkuntran.S.Rajesh,R.S.,"A messy watermarking for medical image Authentication", International Conference on Communications and Signal Processing (ICCSP), Feb. 2011, pp. 418 - 422.

[14] Mona F.M. Mursi, Ghazy M.R. Assassa, Hatim A. Aboalsamh, Khaled Alghathbar. "A Secure Semi-Fragile JPEG Image Authentication Scheme Based on Discrete Cosine Transform". International Conference on Computing, Engineering and Information 2009, pp. 285 – 291.

[15] Zhenni Peng, Wenbo Liu,"Color image authentication based on spatiotemporal chaos and SVD"Chaos, Solitons & Fractals,Volume 36, Issue 4, May 2008, pp. 946-952.

[16] un-Chou Chuang , Yu-Chen Hu, "An adaptive image authentication scheme for vector quantization compressed image", *Elsevier* Journal of Visual Communication and Image Representation, Volume 22, Issue 5, July 2011, pp. 440-449.