

AIVP

ADVANCES IN IMAGE AND VIDEO PROCESSING



TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD	I
DISCLAIMER	II
Bengali Printed Character Recognition Using A Feature Based Chain Code Method	1
Ankita Sikdar	
Sreeparna Banerjee	
Payal Roy	
Somdeep Mukherjee	
Moumita Das	
A Novel Framework for Information Hiding and Image Encryption using Least Significant Bit Techniques	10
H.B.Kekre	
Tanuja Sarode	
Pallavi N. Halarnkar	
On Integration of Error Concealment and Authentication in JPEG2000 Coded Images	26
Qurban A Memon	

EDITORIAL ADVISORY BOARD

Dr Zezhi Chen

Faculty of Science, Engineering and Computing; Kingston University London
United Kingdom

Professor Don Liu

College of Engineering and Science, Louisiana Tech University, Ruston,
United States

Dr Lei Cao

Department of Electrical Engineering, University of Mississippi,
United States

Professor Simon X. Yang

Advanced Robotics & Intelligent Systems (ARIS) Laboratory, University of Guelph,
Canada

Dr Luis Rodolfo Garcia

College of Science and Engineering, Texas A&M University, Corpus Christi
United States

Dr Kyriakos G Vamvoudakis

Dept of Electrical and Computer Engineering, University of California Santa Barbara
United States

Professor Nicoladie Tam

University of North Texas, Denton, Texas
United States

Professor Shahram Latifi

Dept. of Electrical & Computer Engineering University of Nevada, Las Vegas
United States

Professor Hong Zhou

Department of Applied Mathematics Naval Postgraduate School Monterey, CA
United States

Dr Yuriy Polyakov

Computer Science Department, New Jersey Institute of Technology, Newark
United States

Dr M. M. Faraz

Faculty of Science Engineering and Computing, Kingston University London

United Kingdom

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone's views or feelings etc.

Bengali Printed Character Recognition Using A Feature Based Chain Code Method

Ankita Sikdar¹, Sreeparna Banerjee^{2*}, Payal Roy¹, Somdeep Mukherjee¹, and Moumita Das¹

¹Department of Computer Science and Engineering, West Bengal University of Technology, Kolkata, West Bengal, India and ²Department of Natural Science, West Bengal University of Technology, Kolkata, West Bengal, India.

ankita.sikdar@gmail.com, sreeparnab@hotmail.com

ABSTRACT

Bengali, one of the official languages of the Indian subcontinent, is composed of 50 alphabets, of which 11 are vowels and 39 consonants. In addition, Bengali words are formed from compound characters and modifiers. Compound characters are formed by combining parts of single characters and modifiers are parts of vowels and consonants which make sense only when adjacent to or attached with a letter. In this paper, features of Bengali characters are studied using a hierarchical structure. The first few layers deal with features that broadly classify the characters into small size groups. The lower level features are more specific to each character within a group. Higher level features can be identified based on pixel density and arrangement, while the lower level features have been identified using a chain code technique. The algorithm progresses successively through each group in the hierarchy until it finds a match with the input character.

Keywords: Bengali character recognition, feature identification, chain code technique

1 INTRODUCTION

With the rapid proliferation of Internet and Mobile Computing in our daily lives, digitization of text for the purpose of storing and transmitting text across networks has become an absolute necessity. In order to perform digitization, Optical Character Recognition (OCR), both for handwritten and printed text, is required. OCR has thus become an active research area for document analysis and retrieval in different languages. Bengali is one of the official languages of India and the official language of Bangladesh. Hence, OCR in Bengali is also an important step in the digitization of Bengali printed characters processing applications also, the identification of the characters helps In knowing the text and using that information for further processing. A detailed description of its uses is described in [1].

A description of the research work carried out to identify printed characters and a discussion has been provided in [2]. In this paper we have used a chain code [3,4,5] based feature extraction method.

A comprehensive study for feature extraction has been presented in [6]. The feature extraction method that we present in this paper uses a hierarchical scheme. At first a feature set that introduces us to the features of the characters in a hierarchical manner is designed, with the top three levels being the basic features for all the characters and the later levels constitute those features that are particular to a character, thereby providing a robust method for the classification of features that is invariant to the different shapes or sizes of the characters. We then create a database, where we store the chain codes for these lower level features. Now, when an input character is to be identified, we first find out what basic features does it have. This can be done using simple techniques of calculating row and/or column densities, pixel connectivity. Depending on the path in the hierarchy that the character follows, a lower level specific feature is identified. This is done using chain code techniques, which follows the shape of the character. In this method, we propose that the hierarchy should be followed in strict order. If a match with the first group is not found, then algorithm should proceed to the next group in the same hierarchical level. However, if a match is found in one group, the algorithm should proceed down to the next hierarchical level within that group. This paper is outlined as follow. Section 2 presents the hierarchical classification of features. Section 3 describes the database which contains chain code of the features with which the input character is to be matched. Section 4 presents the stepwise algorithm for our method. Section 5 describes the procedure in details followed by an illustration. Section 6 shows the different types of test inputs followed by the results and discussions. Section 7 gives a conclusion and future research scope of our work.

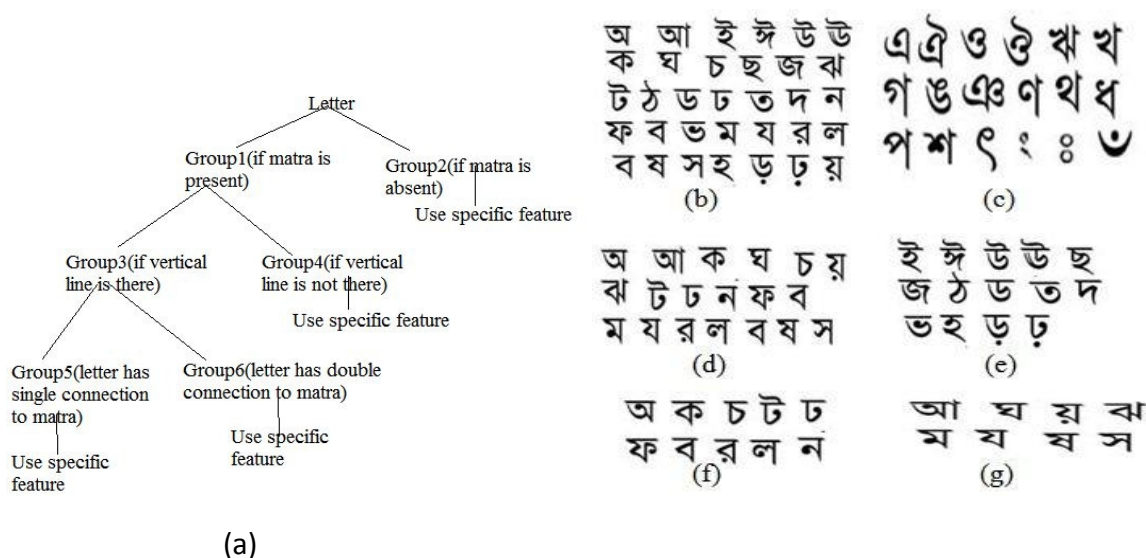


Figure 1: (a): Hierarchy, (b)-(g): Groups 2-6

Figure 1 (a) represents the hierarchical classification scheme. Figure 1(b) depicts the presence of “matra” labelled as Group 1, while Figure 1 (c) represents Group2 - absence of “matra”. Figure 1 (d) denotes Group3 : presence of vertical line, while Figure 1(e) is Group 4- absence of vertical line. Figure 1(f) is Group 5 which has single connectivity to “matra” and Figure 1(g) and Group 6 shown in Figure 2 denotes double connectivity to “matra”.

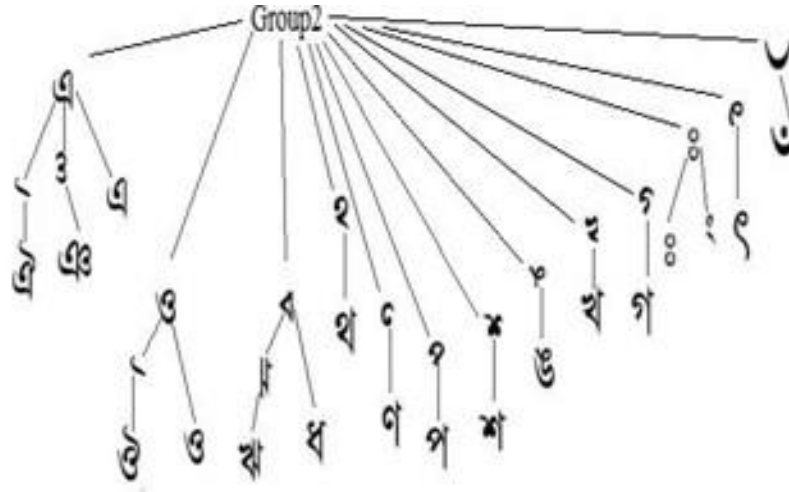


Figure.2: Group 2

After further subdivision, classification based on specific features is shown in Figures 2-5 with Figure 2 labeled as Group 2, Figure 3 is Group 4 , Figure 4 is Group 5 and Figure 5 is Group 6. All these groups have been further subdivided based on specific features as depicted in figures.

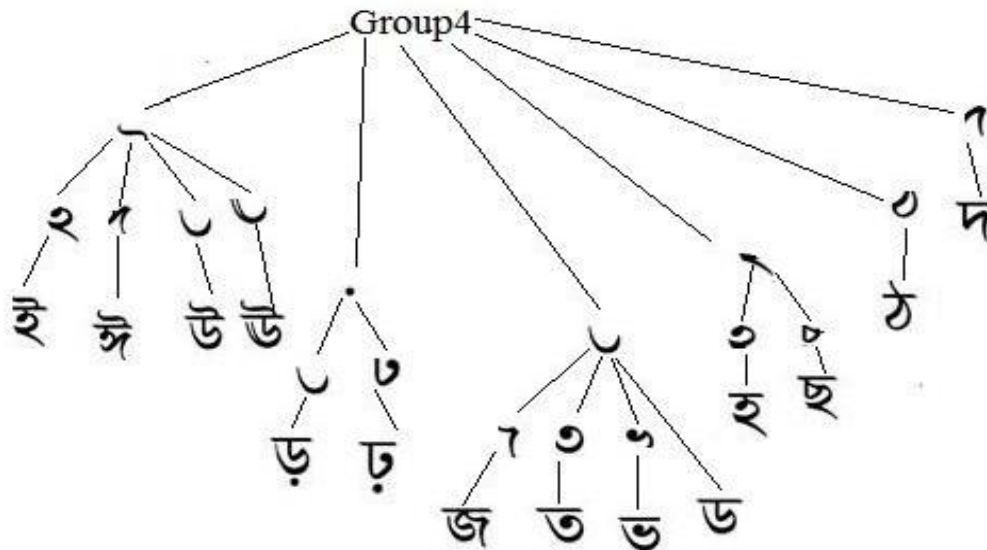


Figure 3: Group 4

2 FEATURE EXTRACTION

Feature extraction is the crucial first step of character identification in our proposed algorithm. Classification starts with the detection of the “matra” (the horizontal headline over some of the characters) in the character. Based on this detection,,group1 and group2, respectively, are defined.

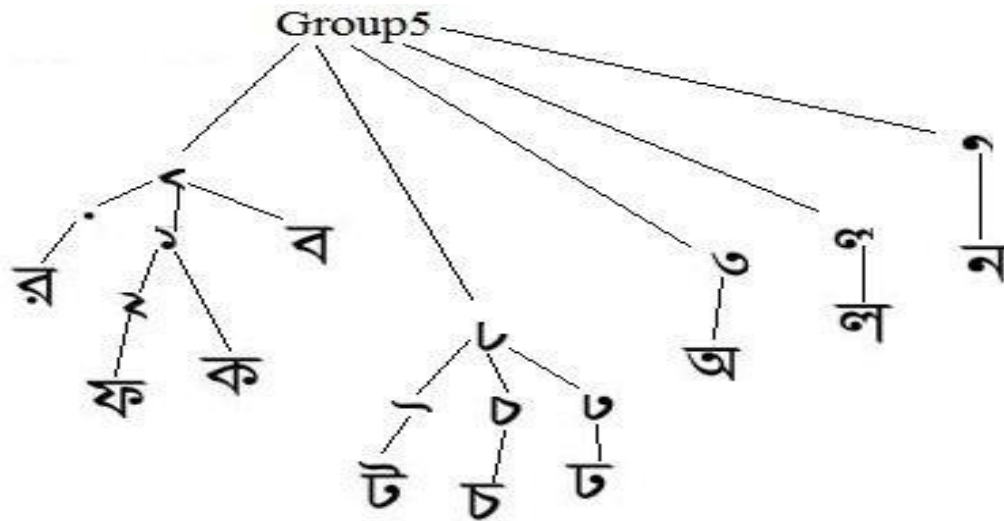


Figure 4: Group 5

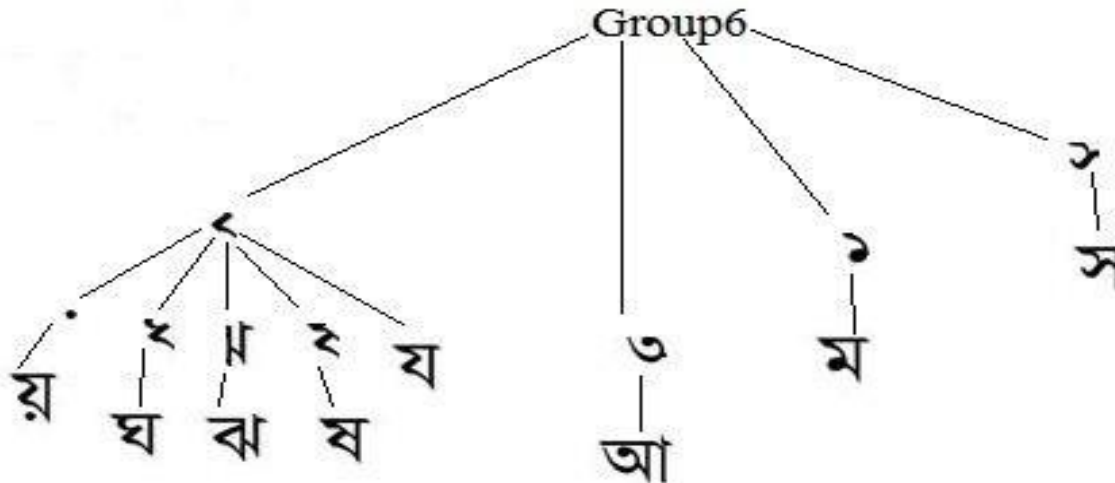


Figure 5: Group 6

The characters in group 1 can be further subdivided into group3 and group4 based on the presence or absence of a vertical line either in the beginning or at the end of the character. Further, the characters in group3 can be subdivided based on the number of places where the “matra” is connected to the character below it. Then, group 5 is defined representing characters having single connectivity to “matra” and group 6 is defined representing characters having

double connectivity to the “matra”. Thus, the basic features which divide the character set into similarly sized groups at each level of the hierarchy have been identified. Now, the characters in the groups which are at the leaf level will need to be identified based on specific features of the particular character. Thus, for each character, features exclusively identifying the character within that group have been defined. The features used to classify each of group 1 to group 6 are labelled as the higher level basic features and the features used in the rest of the hierarchy are labelled as the lower level specific features. The full classification is shown in Figure 6.

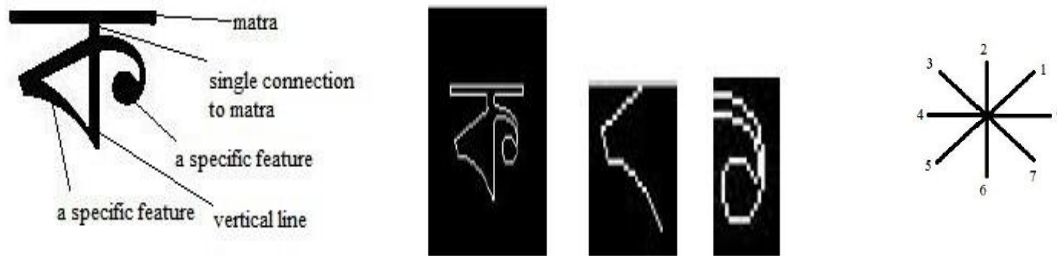


Figure 2: Steps of the method

3 DATABASE

The lower level specific features discussed in section 2 are such features that can directly identify which character it represents within a particular subgroup. In order to train the computer to identify these features in a given input image, the chain code representation for each such feature is determined. The chain code is obtained from the contour representation of the feature and is stored in the database. This representation is to be used later to find a match with the character’s chain code representation.

4 ALGORITHMS

The algorithm is presented as follows:





1. Obtain the input character in RGB form and scale the image to a predefined size.
2. Use Otsu’s method to find out the global threshold for the image.
3. Using this threshold, convert the image to logical form.
4. If the background pixels are white, that is represented by logical ‘1’, then complement the image so that the background pixels are represented by logical ‘0’, else go to step 5.
5. Check to see if the character has a “matra” or not. If yes, then put it in group 1 and proceed to step 6 else put it in group 2 and proceed to step 8.

6. Check to see if the character has a vertical line in the beginning or end of the character or not. If yes, then put it in group 3 and proceed to step 7 else put it in group 4 and proceed to step 8.
7. Check to see if the character is connected to the “matra” at one point or at two points. In the former case, put it in group 5 and proceed to step 8 and in the latter case, put it in group 6 and proceed to step 8.
8. Now, the character could be in either of group 2, group 4, group 5 or group 6. Find out the chain code for the contour of the character.
9. For each group, check in order as shown in the feature classification hierarchy, if the chain code of the features for that group which is stored in the database are found in the chain code for the character contour obtained in step 8.
10. If a match is found then proceed downwards to the group in the next hierarchical level until the character is identified and go to step 11 else proceed to the next group in the same hierarchical level to find out if the character can belong to that group and go to step 9.
11. Algorithm ends.

5 METHODOLOGY

When the input image is obtained in the RGB format, scaling operations on the image are first performed so that the image is of the standard size which has been used in this method. This is followed by converting it to logical form by using Otsu’s global threshold method [7]. If necessary, the complement of the image is found so that the background pixels are represented by ‘0’ and the foreground pixels are represented by ‘1’. Now, the character is identified. Following the hierarchical order, a check is made to see if the character has a “matra” or not. This can be checked by the fact that the identified rows in the image corresponding to the “matra” will have a relative density greater than or equal to 70%. Thus the character can fall in either group1 or group 2 depending on whether the “matra” is present or not respectively.

Now, for characters in group 1, a check can be made to see if there is a vertical line in the beginning or end of the character. This can similarly be checked, because the columns representing such a line would have a relative density greater than or equal to 70%. Thus the character can fall in group 3 or group 4 depending on the presence or absence of the vertical line respectively. The characters of group 3 can be further checked to see the connectivity to the “matra”. The character below the “matra” is joined to it either at one point or two points. The width of the connection is also very small, less than 5% of the total number of pixels in the row. Thus the character can fall in group 5 or group 6 depending on whether the character has a single connection to the “matra” or double












The second feature at the same level is  . The chain code for this feature is 0000070077077667 6666 6656555 44444323222 2110000777 122232334 34434 444. Now this pattern can be found in the chain code for the character and a match is found. Then proceed downwards into the subgroup. The first feature encountered is  . The chain code representation for this feature is 000007776555570707634344 34231 101133443. However, such a pattern in the chain code for the character  is not found and since there are no other options left, therefore this character has to be the other one in that subgroup and so this method has correctly identified the character as .

6 RESULT AND DISCUSSIONS

A large number of samples for each character have been collected [9] and tested using the proposed method. The results for the experiment are given in Table 1.

It is seen from the results, that the chain code matching algorithm gives a high accuracy of matched characters. The chain code follows the direction that the characters take, encoding the shape of the desired feature. Using a variety of images, where the characters may be represented in various fonts and sizes, this approach gives satisfactory results because the chain code will follow the direction of the feature, which will always be same for all cases. The negligible differences that occur have been studied carefully and accounted for. Although Chain code matching technique gives very good results in most of the cases, it is cumbersome to do so for each and every feature and write algorithms for each such feature.

Table 1. Results of the method.

LETTER TAKEN	NUMBER OF SAMPLES TAKEN	PERCENTAGE OF MATCH
	50	98
	50	100
	50	94
	50	92
	50	94
	50	94
	50	94
	50	100
	50	94
	50	98
	50	90

7 CONCLUSION AND FUTURE WORK

Based on the results obtained, it can be concluded that the classification accuracy has been over 90 %, with the best three letters having an accuracy of 100% and 98%. In some cases a character may have been misclassified because the font used did not represent the character in its proper format. It is difficult to account for all the different fonts available for writing Bengali characters. However, the feature classification presented in this paper is based on crucial features that have almost similar representations in every font system. Therefore, this classification is quite robust. The algorithms used to match with the patterns are quite flexible. Although many machine learning based approaches to Bengali character recognition are being attempted, this simple method has its strength in identifying the characters based on certain very crucial characteristics and is thus a very universal approach, which can be extended to Bengali handwritten character identification in the future.

REFERENCES

- [1]. Mohammed Jasim Uddin, Mohammed Towhidul Islam and Md. Abdus Sattar, *Recognition of Printed Bangla Characters Using Graph Theory*, National Conference on Computer and Information System-NCCIS, Dec 9-10, 1997, Dhaka, Bangladesh
- [2]. Chaudhuri, B. B., Pal, U.: A Complete Printed Bangla OCR System. *Pattern Recognition*, Vol. 31. (1998) 531-549
- [3]. Ujjwal Bhattacharya, Malayappan Shridhar, and Swapan K.Parui. On recognition of handwritten bangla characters. In *ICVGIP*, pages 817- 828, 2006.
- [4]. J.U. Mahmud, M.F. Raihan and C.M. Rahman, "A Complete OCR System for continuous Bengali Character", *TENCON 2003, Conference on Convergent Technologies for Asia-Pacific Region*, 15-17 Oct. 2003
- [5]. Dewi Nasien, Habibollah Haron, Siti Sophiyati Yuhaniz, "The Heuristic Extraction Algorithms for Freeman Chain Code of Handwritten Character", *International Journal of Experimental Algorithms-IJEA*, Vol. 1, Issue 1, pages 1-20.
- [6]. Trier, O. D., Jain, A. K. and Taxt, T.: Feature Extraction Methods for Character Recognition - A Survey. *Pattern Recognition*, Vol. 29 (1996) 641 - 662
- [7]. Otsu, N.: A Threshold Selection Method from Grey-Level Histograms. *IEEE Trans. Systems, Man, and Cybernetics*, Vol. 9 (1979) 377-393
- [8]. Freeman, H.: Computer processing of Line-drawing Images *ACM Computing Surveys*, Vol. 6 (1974) 57-97
- [9]. Sikdar A., Roy P., Mukherjee S., Das M. and Banerjee S., A Feature Based Chain Code Method for Identifying Printed Bengali Characters, (2012) *Proceedings, SIPM 2012*, 89-96.

A Novel Framework for Information Hiding and Image Encryption using Least Significant Bit Techniques

H.B.Kekre¹, Tanuja Sarode², Pallavi N. Halarnkar³

^{1,3}MPSTME, NMIMS University, Mumbai;

²TSEC, Mumbai University, Mumbai;

Hbkekke@yahoo.com, Tanuja0123@yahoo.com, Pallavi.halarnkar@gmail.com

ABSTRACT

Security of Digital Images is utmost important. Nowadays not only data but also digital images are increasing in a huge number. Good encryption techniques are always in need. In this paper we have proposed a Novel Framework, which is a combination of Information Hiding and Image Scrambling. The proposed framework is one of its kind and doesn't resemble to any existing frameworks in literature. For Image scrambling R-Prime Shuffle technique has been used.

Keywords: Image security, Information Hiding, Steganography, Image Encryption, Image Scrambling.

1 INTRODUCTION

Data security is important, so is the security of digital images. Some of the existing data security techniques cannot be directly used for securing images. Digital images have huge amount of data which makes some of the existing techniques unsuitable for securing them.

Jarno[1]proposed a modification to the existing least significant matching algorithm. In the existing technique a choice whether to add or subtract 1 is random, however the proposed method uses the choice to set a binary function of two cover pixels to the desired value. The pair of pixels is used as a unit for embedding purpose, the LSB of the first pixel carries one bit of information, and a function of two pixel values carries another bit of information. The proposed method gives the same payload as LSB but with fewer modifications to cover image. The proposed method shows a good performance as compared to LSB in terms of distortion and steganalysis attack.

A novel technique for data hiding based on Fibonacci is proposed in [2]. The method is based on bit plane decomposition for embedding the message. The technique is compared with traditional LSB method for hiding capacity.

Sandipan et al. proposed a data hiding technique[3]using the concept of prime numbers, which is an improvement over Fibonacci LSB method. The technique is based on decomposition of a number in sum of prime numbers. This decomposition generates a different set of virtual planes, suitable for embedding purpose. The proposed technique allows embedding in higher bit planes without much distortion and a good quality stego image is obtained. A comparative analysis between LSB, Fibonacci LSB and the proposed technique is been done. The proposed technique has proved the quality of the stego image to be much better than the other two methods.

Kekre et al. [4] proposed a steganography technique using the concept of Parity. The number of 1's and 0's are balanced by the technique in a such a way that it minimizes the possibility of suspicion. Depending upon the message bit 0/1 , the cover image byte is either modified or kept the same so as the embedding of the message bit should result in the even parity of the cover image byte.

Clandestine Data Entrenching and Salvaging, a information hiding technique was proposed by Kekre et al. [5]. In this paper two techniques are proposed, LSB 2 bit and LSB 3 bit, In the first technique , LSB and next to LSB bit are XORed, depending on the message bit 1/0 the LSB is either changed or kept the same. In the second technique, LSB bit, Next to LSB bit and Next to Next LSB bit is XORed and depending on the value of the message bit LSB is either modified or kept the same.

Information hiding technique is not limited to spatial domain, but they are explored in transform domain also. A LSB steganography technique in DCT domain is proposed by Rajib et al. in [6]. A 8x8 block of DCT coefficients is selected in cover image for embedding the secret message. A variable bit operation is applied to the selected DCT coefficients to embed a byte of secret data, where the variable bit operation is dependent on the value of the pixel. Statistical analysis is performed which shows the method is robust against various steganalysis methods.

Security of digital images is very important , a number of scrambling techniques are proposed which make the visual appearance of the digital image meaningless to the user. Until the method of scrambling is known, the user cannot descramble the digital image for its actual content. One such technique based on extension to queue transformation is proposed by Hai-Yan in [7]. The existing queue transformation technique has many disadvantages which are been overcome in this extension been proposed. The algorithm requires only one step compared to two steps to complete the scrambling. The reference point can change in every stage. To decode the image, the step, reference point all have to be known.

Image scrambling technique based on Arnold transformation is proposed by Min Li et.al in [8]. The proposed technique improves the security of image during transmission. The traditional method based on Arnold applies only to a square area, which is a limitation. This limitation has

been overcome in the proposed method by dividing the image into multiple square areas and applying the transformation for scrambling the image.

Kekre et al. proposed an Image scrambling method using the concept of Relative Prime called as R-Prime shuffle technique for Image scrambling in [9]. The method makes use of correlation concept between the rows and columns of the image. In image scrambling it is required that the correlation between the image rows and columns be minimum so as to make the details of the image unavailable to the user.

The R-Prime shuffle technique was further extended by Kekre et al. on Image blocks [10]. This method was compared to Original R-Prime shuffle on image as a whole. The method is difficult to decode as compared to original method as every block of the image has a different prime rows and columns considered for shuffling based on their correlation.

Tan Yongjie et al. [11] proposed a new method for evaluating the degree of scrambling using the grey relation analysis theory. The scrambled image is firstly analyzed so also its histogram. The scrambled image is then sub divided into sub images to construct some histogram sequences and make them small sequences. The grey relevancy of every two sequences using grey relation analysis is calculated to evaluate the image scrambling degree.

Zhang et al. proposed a Digital image encryption technique based on chaos and improved DES in [12]. The method makes use of Logistics chaos sequencer to generate pseudo random sequences, this sequence is carried on RGB image chaotically, then a double time encryption with improved DES is applied. Analysis indicate that the method is sensitive to initial condition and has high security and encryption speed.

Mohammed et al.[13] proposed a Image encryption scheme using Lagrange-Least squares Interpolation. The method consists of two main parts, Encryption/Decryption and ciphered key. The XOR operator is used in the diffusion stage to modify the pixel value which is spread to all the pixels in the image. In the substitution stage two encryption processes are used, Lagrange Process and Least square process. The decryption is just the reverse of the encryption method. The proposed system makes use of a key of length 192 bits (24 bytes). The key is expanded using AES-192 key expansion algorithm. The second approach makes use of an image as a key to cipher the plane image and the key used is expanded using CBI key expansion algorithm.

Various Encryption schemes have been compared based on a number of parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed and cryptographic security in [14]. The encryption techniques compared are from spatial as well as frequency domain. The conclusion says that none of techniques satisfies all the considered parameters for comparison.

An image security technique using the permutation of RGB components is proposed in [15]. Data bits from a textual message are encrypted using some key to some suitable non linear pixels and bit positions about the entire image. The resultant is a watermarked image. After this, three different image shares using any two components of R G and B of the watermarked image is formed. Similarly the key is also divided into three different shares and assigned to image shares.

A hybrid approach for Image security combining image encryption and steganography is proposed by Jaspal Kaur et al. in [16]. The image is firstly encrypted using modified AES algorithm then it is hidden into the cover image using the concept of steganography. The experimental results show that the hybrid method provides greater security against attacks.

Kekre et al.[17] proposed a Digital encryption method using the Random discrete distributions and MOD operator. In this paper a new parameter called as PAFCPV(Peak Average Fractional Change in Pixel Value) is proposed which gives an analysis of how good is the encryption method. The range of this parameter is between 0 to 1, where 0 means the image value is not disturbed and 1 indicates the every bit of the pixel value is affected by the encryption method.

Somdip Dey proposed a method called as SD-AEI which is an improvement over SD-EI in [18]. In the first stage every pixel value is converted to binary, equivalent to the length of the password the bits are rotated and then reversed. In the second stage the extended hill cipher technique is applied by using involuntary matrix which is generated by the same password as the first stage. In the final stage the whole image is randomized using Modified MSA Randomization encryption technique; this randomization is dependent on a unique number. The proposed method is very effective in encrypting any type of images.

2 PROPOSED INFORMATION HIDING FRAMEWORK

In this paper, a Novel Information Hiding framework is proposed. The steps of the framework are as follows

- 1) Take the cover image of size x bytes
- 2) Apply the scrambling Algorithm,(R-Prime shuffle), a scrambled image is obtained
- 3) To hide the message image use LSB technique(LSB 1 Bit, 2 Bit, 3 Bit and Parity), a scrambled stego image is obtained
- 4) The scrambled stego image obtained in step 3, apply descrambling algorithm to get a innocent stego image.

Note: The message image is hidden in the scrambled image, this scrambled stego image is now descrambled so as to obtain an innocent stego image which can be transferred across the network. Now some intruder tries to intercept the message from the innocent stego image, he

will obtain an encrypted message image which will be difficult to decrypt and get some useful information out of it. This can be seen from the experimental results obtained below.

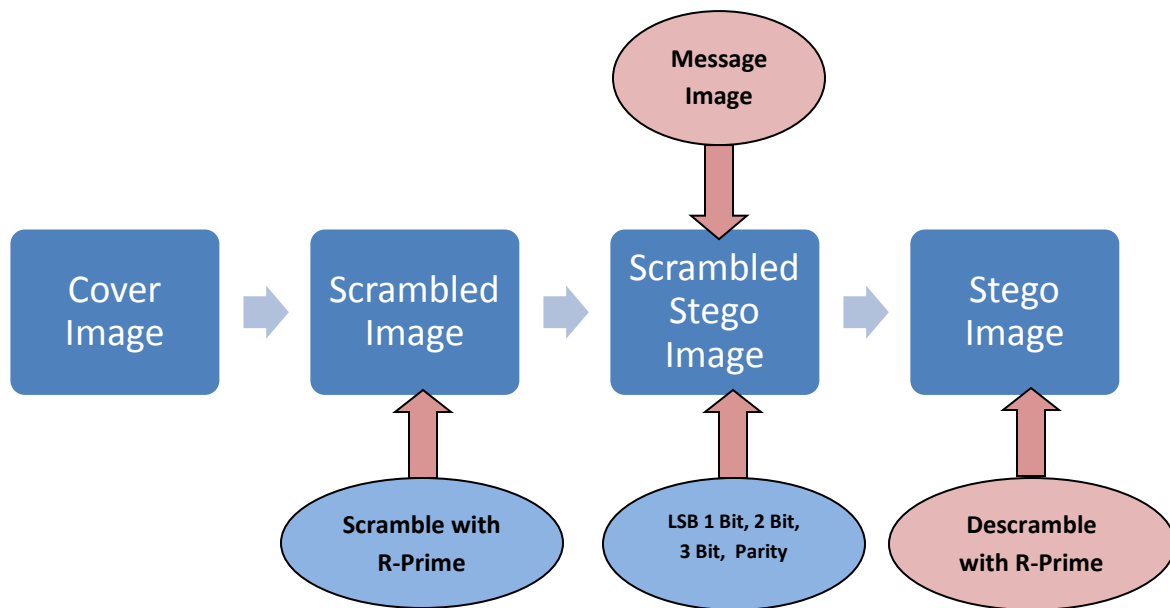


Figure 1. Embedding Stage

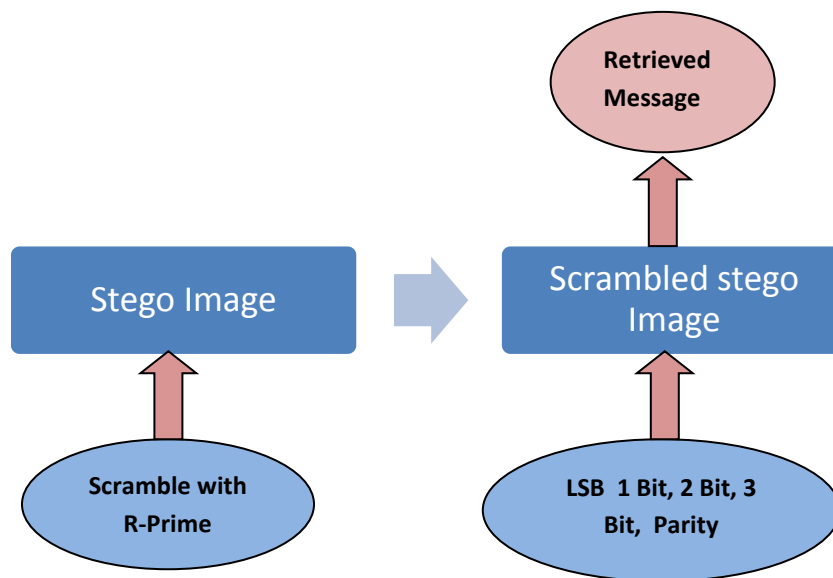


Figure 2. Retrieving Stage

2.1 R-Prime Shuffle [9]

Scrambling

The method used for Encryption is as follows

- Read the image

- Based on the Size of the Image(MXN), find out all the Relative Prime Numbers and save them in a set S
- Using set S to find the correlation of the First row with remaining rows (positions w.r.t elements present in the set).
- Consider the lowest correlation as the key to shuffle the rows in the image
- Continue till all the positions in the image are considered
- Save the Relative Primes Numbers as a key considered for Row and Column Shuffling

Repeat the same procedure for Column shuffling

Descrambling

- Use the Saved key for Row and Column Shuffling to get the Original Image back
- Use the column Relative Prime and rearrange the columns, this will give row shuffled image
- Using this row shuffled image and the key for row relative prime rearrange the rows which will give you Original Image back.
- Continue till all the positions in the image are rearranged

2.2 LSB 1-Bit Technique

Embedding Algorithm

- Take message image with size x bytes
- Cover image size should be at least 8 times x.
- Extract RGB components of pixel intensity values of message and the cover image
- Take the successive R, G, and B component values of pixels and convert them into array of values for messages and the cover image.
- Convert every decimal value into 8 bit binary equivalent for cover and message images.
- Every message bit is embedded into LSB's of the cover image.

Retrieving Algorithm

The message retrieving is done as per the algorithm given below

- Take stego image with size x bytes
- Extract R, G, B Components of pixel intensity values of stego image.
- Take successive R, G, B component values of pixels and convert them into array of values for stego image.

- Convert every decimal value into 8 bit binary equivalent for stego image.
- Retrieval of the message bit is done by extracting the LSB of every pixel from the Stego image of the R, G and B component.

2.3 Using 2 LSB's and Using 3 LSB's [5]

The technique implemented in this section just does not replace the LSB, but the LSB is modified by taking into consideration the data bits of the message, the cover image LSB and the other bits of the cover image as well. Advantages of this method are its encoding / decoding complexity is less, cover capacity is same as LSB, accuracy of retrieval is 100%, and good perceptual transparency of cover image.

Embedding Algorithm

- Take message image with size x bytes
- Cover image size should be at least 8 times x.
- Extract RGB components of pixel intensity values of message and the cover image
- Take the successive R, G, and B component values of pixels and convert them into array of values for messages and the cover image.
- Convert every decimal value into 8 bit binary equivalent for cover and message images.
- Every message bit is embedded into LSB's of the cover image after processing.
- Processing is done as follows
- If the message bit to be embedded is 0, then adjust the LSB such that the XOR ing of LSB and next to LSB is 0 and if the message bit to be embedded is 1, then adjust the LSB such that the XOR ing of LSB and next to LSB is 1 if LSB-2 bit method is being used
- If the message bit to be embedded is 0, then the LSB is adjusted such that the XOR ing of LSB next to LSB and next to next to LSB is 0. And if the message bit to be embedded is 1, then adjust the LSB such that the XOR ing of LSB next to LSB and next to next to LSB is 1 if LSB-3 bit method is being used
- Convert every 8 bits into byte for the cover image
- Take 3 bytes and group them as 3 RGB components of a 1 pixel. Perform this step for the full cover image.
- The message embedding in the cover image is over.

Retrieving Algorithm

The message retrieving is done as per the algorithm given below

- Take stego image with size x bytes
- Extract R, G, B Components of pixel intensity values of stego image.
- Take successive R, G, B component values of pixels and convert them into array of values for stego image.
- Convert every decimal value into 8 bit binary equivalent for stego image.
- Retrieval of the message bit is done by XOR ing the LSB and Next to LSB. If it is 1 then message bit is 1. If it is 0 then message bit is 0. For LSB-3 bit method, Next to Next to LSB is XOR ed.
- Convert every 8 bits into byte for the message.
- Take 3 bytes and group them as 3 RGB components of 1 pixel. Perform this step for the full message
- The message retrieval is over

Table No 1. Truth Table for LSB 2 Bit Method

LSB	Next to LSB	Message Bit	LSB Adjusted
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Table No 2. Truth Table for LSB 3 Bit Method

Next to Next LSB	Next to LSB	LSB	Message Bit	LSB Adjusted
0	0	0	0	No change
0	0	1	0	0
0	1	0	0	1
0	1	1	0	No change
1	0	0	0	1
1	0	1	0	No Change
1	1	0	0	No Change
1	1	1	0	0
0	0	0	1	1
0	0	1	1	No Change
0	1	0	1	No Change
0	1	1	1	0
1	0	0	1	No Change
1	0	1	1	0
1	1	0	1	1
1	1	1	1	No Change

2.4 Considering Parity [4]

For embedding any message image with size x bits, the cover image size should be at least x bytes. Extract the R, G, B components of the pixels, and each byte will be used to embed 1 secret message bit. Every bit of the message to be embedded is taken one at a time. To embed this bit one byte of the cover image is taken. Depending upon the value of the message bit to be embedded is 0, the LSB of the cover image byte is modified or kept same such that the parity of the cover image byte after this message bit is embedded is even. Also if the message bit to be embedded is 1, then the LSB of the cover image byte is modified or kept same such that the parity of the cover image byte after this message bit is embedded is odd

For retrieving the message the stego image(image which contains the embedded message) is taken. The parity of every byte is checked. If the parity is even that means the message bit is 0 and if the parity is odd it means the message bit is 1.

In this way after 8 such message bits are retrieved they are converted to decimal and this decimal number becomes the intensity value of the first message pixel. This procedure is repeated until the full message is retrieved, and the message image is formed.

3 EXPERIMENTAL RESULTS

For Experimental purpose , five different 24-bit color images of size 256X256 were used for all the four methods , LSB 1-Bit, LSB 2-Bit, LSB 3-Bit and LSB Parity.

3.1 LSB 1-Bit

The results obtained from the proposed framework for LSB 1 Bit and displayed below. Figure 3(a) shows the original Image, 3(b) shows the scrambled image obtained after applying R-Prime Shuffle Technique, 3(C) shows the scrambled stego image obtained after embedding atm image using LSB 1 Bit method. This scrambled stego image is now converted to innocent stego image by descrambling which is seen in 3(d).

The advantage of the proposed framework can be seen from Figure.4. Figure 4(a) shows the original message image, 4(b) shows the encrypted message image obtained if some intruder tries to get it from the innocent stego image. 4(c) show the retrieved message image from the scrambled stego image.

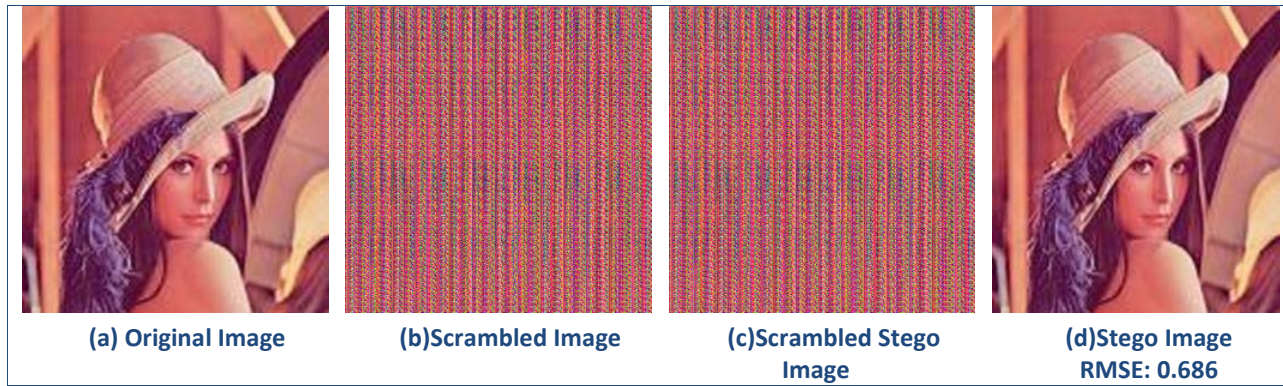


Figure. 3



Figure. 4

3.2 LSB 2-BIT

The results obtained for LSB 2 Bit are displayed below. Figure 5(a) shows the original Image, 5(b) shows the scrambled image obtained after applying R-Prime Shuffle Technique, 5(c) shows the scrambled stego image obtained after embedding atm image using LSB 2 Bit method. This scrambled stego image is now converted to innocent stego image by descrambling which is seen in 5(d).

Figure 6(a) shows the original message image, 6(b) shows the encrypted message image obtained if some intruder tries to get it from the innocent stego image. 6(c) show the retrieved message image from the scrambled stego image.

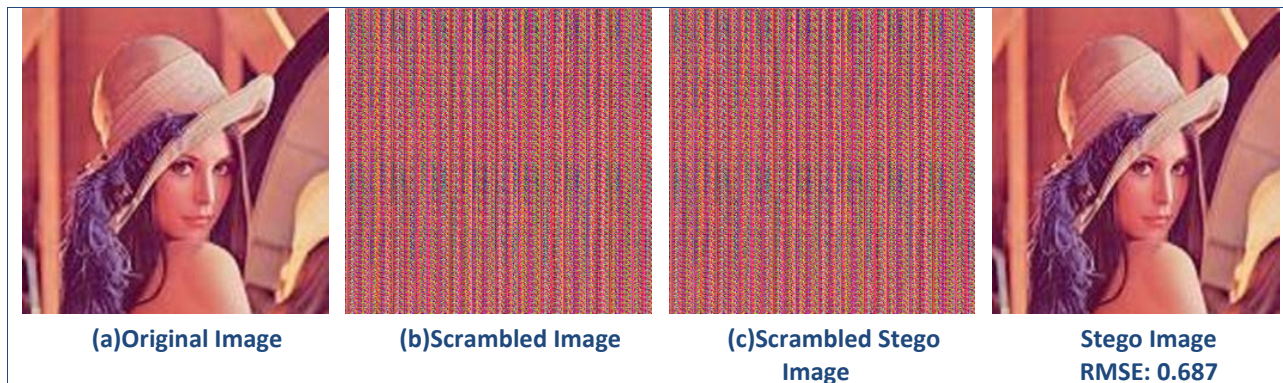


Figure 5.



Figure 6

3.3 LSB -3 BIT

The results obtained for LSB 3 Bit and displayed below. Figure 7(a) shows the original Image, 7(b) shows the scrambled image obtained after applying R-Prime Shuffle Technique, 7(c) shows the scrambled stego image obtained after embedding atm image using LSB 3 Bit method. This scrambled stego image is now converted to innocent stego image by descrambling which is seen in 7(d).

Figure 8(a) shows the original message image, 8(b) shows the encrypted message image obtained if some intruder tries to get it from the innocent stego image. 8(c) show the retrieved message image from the scrambled stego image.

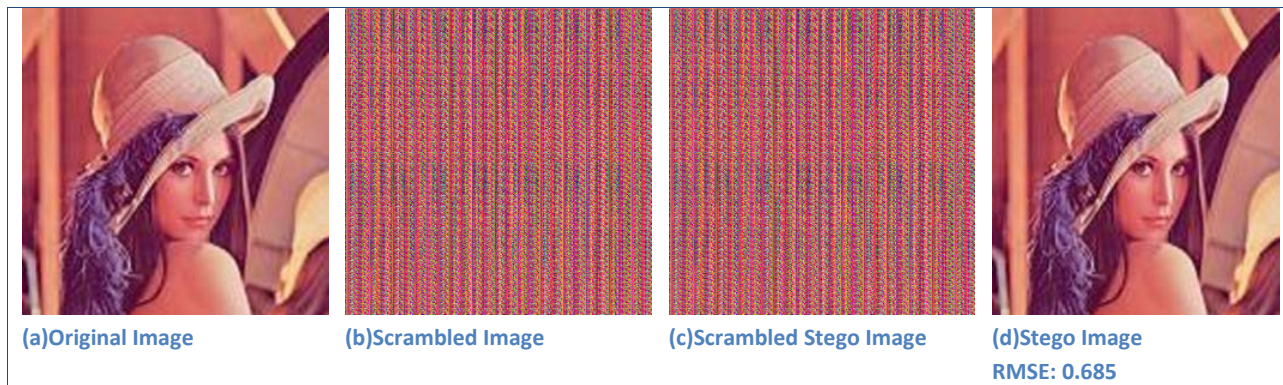


Figure 7.



Figure. 8

3.4 LSB PARITY

The results obtained for LSB Parity and displayed below. Figure 9(a) shows the original Image, 9(b) shows the scrambled image obtained after applying R-Prime Shuffle Technique, 9(c) shows the scrambled stego image obtained after embedding atm image using LSB Parity

method. This scrambled stego image is now converted to innocent stego image by descrambling which is seen in 9(d).

Figure 10(a) shows the original message image, 10(b) shows the encrypted message image obtained if some intruder tries to get it from the innocent stego image. 10(c) shows the retrieved message image from the scrambled stego image.

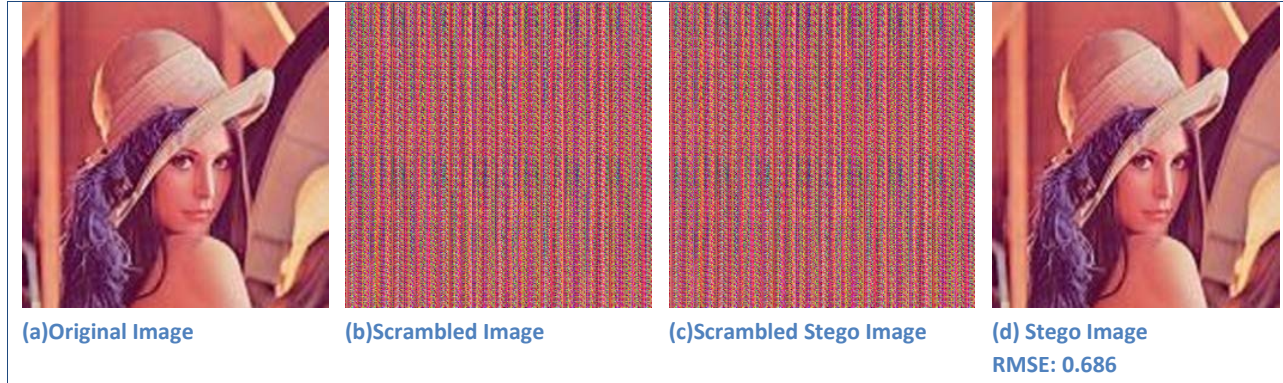


Figure. 9

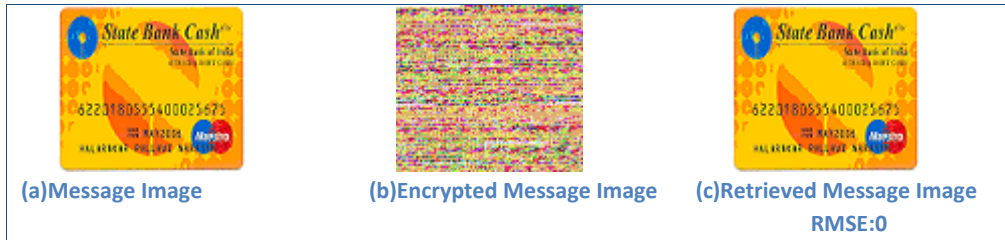


Figure. 10

Table No 3 gives the values obtained for Average Correlation between rows and columns of five scrambled images of size 256X256 for LSB 1-Bit, LSB 2-Bit, LSB 3-Bit and LSB Parity method. The original image correlation is also given for the respective images. It can be observed that for all the images and different LSB methods , the correlation is reduced. The table also displays values obtained for Average Moving Distance Maximum(AMD- Max) for an image of size 256X256,the AMD obtained by the scrambling technique R-Prime shuffle and Distance scrambling factor[8].

Table 3.Values of Average correlation between rows and columns of original image and scrambled image, Average Moving Distance and Distance Scrambling factor between original image and scrambled image

Lena Image Rows: 0.8454 Cols: 0.7005	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
Avg Corr Rows	0.306			
Avg Corr Cols	0.268			
AMD(Max)	360.62			
AMD	136.48			
DSF	0.378			

Kutub Image Rows: 0.2784 Cols: 0.3896	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
Avg Corr Rows	0.181			
Avg Corr Cols	0.187			
AMD(Max)	360.62			
AMD	133.58			
DSF	0.370			

Vegetable Image Rows: 0.5176 Cols: 0.4994	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
Avg Corr Rows	0.199			
Avg Corr Cols	0.190			
AMD(Max)	360.62			
AMD	132.10			
DSF	0.366			

Baboon Image Rows: 0.4355 Cols: 0.5276	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
Avg Corr Rows	0.185			
Avg Corr Cols	0.192			
AMD(Max)	360.62			
AMD	130.44			
DSF	0.361			

Fruits Image Rows: 0.6203 Cols: 0.6317	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
Avg Corr Rows	0.196			
Avg Corr Cols	0.213			
AMD(Max)	360.62			
AMD	133.26			
DSF	0.369			

Table No 4 gives the values of RMSE, PSNR obtained for stego image using LSB 1-Bit , LSB 2-Bit, LSB 3-Bit and LSB Parity.

Table 4. Values of RMSE, PSNR, between original Image and Stego image

Lena	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
RMSE	0.686	0.687	0.685	0.686
PSNR	51.39	51.38	51.40	51.40
Kutub	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
RMSE	0.685	0.685	0.685	0.684
PSNR	51.41	51.40	51.41	51.42
Vegetable	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
RMSE	0.684	0.687	0.686	0.685
PSNR	51.42	51.39	51.40	51.41
Baboon	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
RMSE	0.685	0.687	0.686	0.686
PSNR	51.40	51.38	51.40	51.39
Fruits	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
RMSE	0.684	0.686	0.686	0.687
PSNR	51.41	51.40	51.40	51.38

Table No 5 gives the values of PAFCPV and NPCR obtained for encrypted message image using LSB 1-Bit , LSB 2-Bit, LSB 3-Bit and LSB Parity

Table 5. Values of PAFCPV and NPCR, between original Message Image and Encrypted Message image

Lena	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
PAFCPV	0.316	0.316	0.316	0.316
NPCR	99.34	99.35	99.34	99.36
Kutub	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
PAFCPV	0.306	0.305	0.306	0.305
NPCR	97.91	97.83	97.87	97.86
Vegetable	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
PAFCPV	0.397	0.398	0.398	0.397
NPCR	99.39	99.39	99.38	99.40
Baboon	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
PAFCPV	0.297	0.297	0.297	0.296
NPCR	98.89	98.88	98.86	98.88
Fruits	LSB 1 Bit	LSB 2 Bit	LSB 3 Bit	LSB Parity
PAFCPV	0.325	0.325	0.325	0.324
NPCR	99.09	99.11	99.08	99.08

4 OBSERVATIONS

It can be observed from the experimental results the maximum reduction in the correlation for rows is obtained in fruits image where the correlation is reduced by 68.41 %. Minimum column correlation is obtained in fruits image with a reduction in column correlation by 66.29%. DSF is maximum for Lena image. Mean squared error obtained for all the stego images is approximately the same so also is the PSNR for all the methods of LSB. The encrypted message image obtained for Vegetable image gives a good value for PAFCPV. The NPCR value obtained incase of Kutub Minar image is less as compared to other images.

5 CONCLUSION

In this paper, we have proposed a Novel Approach for securing the message image. A lot of Information hiding techniques are proposed in literature, they make use of existing encryption methods to encrypt the message image and then embed it in the cover image to create a stego image which can be transferred, here our framework uses completely a different approach, using a simple scrambling technique, we a getting a good encrypted message image from a stego image which will be difficult to decrypt.

REFERENCES

- [1]. Mielikainen, Jarno. *LSB matching revisited*. Signal Processing Letters, IEEE 13, no. 5 (2006) .p. 285-287.
- [2]. Battisti, F., M. Carli, A. Neri, and K. Egiazarian. *A Generalized Fibonacci LSB Data Hiding Technique*. Computers and Devices for Communication (CODEC-06), Institute of Radio Physics and Electronics, University of Calcutta International Conference on. 2006.
- [3]. Dey, Sandipan, Ajith Abraham, and Sugata Sanyal. *An LSB data hiding technique using prime numbers*. In *Information Assurance and Security, 2007. IAS 2007. Third International Symposium on*,. IEEE, 2007. p. 101-108
- [4]. Kekre, H. B., and Archana A. Athawale. *Personal Data Ingrain and Regain*,. NCA, FCRCE, Bandra (W), Mumbai, 16th-17th May (2008).National Conference on Algorithms p. 88-93
- [5]. Kekre, H. B., Archana A. Athawale, and Sudeep D. Thepade. *Clandestine Data Entrenching and Salvaging*. In *National Conference on Information and Communication Technology 29th Feb and 1st Mar, NCICT-08*.p. 1-7
- [6]. Biswas, Rajib, Sayantan Mukherjee, and Samir Kumar Bandyopadhyay. *DCT Domain Encryption in LSB Steganography*. In *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*,. IEEE, 2013. p. 405-408
- [7]. Zhang, Hai-Yan. *A new image scrambling algorithm based on queue transformation*. In *Machine Learning and Cybernetics, 2007 International Conference on*, vol. 3, IEEE, 2007. p. 1526-1530.

- [8]. Li, Min, Ting Liang, and Yu-jie He. *Arnold Transform Based Image Scrambling Method*. Multimedia Technology (ICMT 2013) International Conference on .2013. p.1309-1316
- [9]. Kekre, H. B., Tanuja Sarode, and Pallavi Halarnkar. *Image Scrambling using R-Prime Shuffle*. IJAREEIE, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.2013. 2(8). p.4070-4076
- [10]. Kekre, H. B., Tanuja Sarode, and Pallavi Halarnkar. *Image Scrambling using R-Prime Shuffle on Image and Image Blocks*. IJARCCCE. International Journal of Advanced Research in Computer and Communication Engineering. 2014. 3(2). p.5471-5476.
- [11]. Yongjie, Tan, and Zhou Wengang. *Image scrambling degree evaluation algorithm based on grey relation analysis*. In Computational and Information Sciences (ICCIS), 2010 International Conference on, IEEE, 2010 p. 511-514.
- [12]. Yun-Peng, Zhang, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan, and Dai Wei-di. *Digital image encryption algorithm based on chaos and improved DES*. In Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, IEEE, 2009.p. 474-479.
- [13]. Shreef, Mohammed A., and Haider K. Hoomod. *Image Encryption Using Lagrange-Least Squares Interpolation*. (IJACSIT). International Journal of Advanced Computer Science and Information Technology. 2013 2(4).p. 35-55.
- [14]. Shah, Jolly, and Vikas Saxena. *Performance Study on Image Encryption Schemes*. (IJCSI) International Journal of Computer Science. 2011. 8(4).p.349-355.
- [15]. Samanta, Sabyasachi, Saurabh Dutta, and Goutam Sanyal. *An enhancement of security of image using permutation of RGB-components*. In Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol. 2, IEEE, 2011. p. 404-408.
- [16]. Saini, Jaspal Kaur, and Harsh K. Verma. *A hybrid approach for image security by combining encryption and steganography*. In Image Information Processing (ICIIP), 2013 IEEE Second International Conference on, IEEE, 2013. p. 607-611.
- [17]. Kekre, H. B., Tanuja Sarode, and Pallavi Halarnkar. *Performance Evaluation of Digital Image Encryption Using Discrete Random Distributions and MOD Operator*. IOSR-JCE. IOSR Journal of Computer Engineering. 2014. 16(2).Ver V. p.54-68.
- [18]. Dey, Somdip. "SD-AEI: An advanced encryption technique for images." In *Digital Information Processing and Communications (ICDIPC), 2012 Second International Conference on*, pp. 68-73. IEEE, 2012.

On Integration of Error Concealment and Authentication in JPEG2000 Coded Images

Qurban A Memon

Associate Professor, EE department, UAE University, Al-Ain 15551, United Arab Emirates
qurban.memon@uaeu.ac.ae

ABSTRACT

Nowadays, it is widely understood that data compression is not only essential to speed up the transmission rate but also to provide other gains like low storage. In order to counter data manipulations and tampering during transmission, the image authentication has turned out to be equally important. But the drawback of compressed data transmission is that the compressed data are susceptible to channel impairments. In this paper, an error concealment approach is integrated with low cost image authentication scheme to benefit better visual quality as well as content author and user satisfaction. The image authentication includes content based digital signature that is watermarked and diffused in the whole image before JPEG2000 coding. To tackle noise, the error detection and concealment technology is examined to include edge information as part of error concealment approach. The edge image is sent along with JPEG2000 coded image to determine corrupted coefficients. The simulation results are conducted on test images for different values of bit error rate to judge confidence in noise concealment within the received images.

1 INTRODUCTION

The two common standards to compress and code images before transmission and storage are JPEG and JPEG2000. The JPEG standard is based on the discrete cosine transform (DCT) while JPEG2000 is based on the Wavelet transform. JPEG is the older standard and still widely used. The JPEG2000 is the newer standard.

Data compression reduces the use of channel bandwidth; however compressed data are more vulnerable to channel noise. Therefore, the transmitted data must be resilient to channel noise and other impairments due to channel coding of binary bits [1-4]. Several techniques have been proposed in the literature to address the problem of transmission errors by making transmitted data more robust to channel noise and to conceal corrupted data at the receiver. The authors in [5] present a scalable scheme for robust JPEG 2000 images and video transmission to multiple wireless clients, using an adaptive bandwidth estimation tool. In

another research work [6], the authors present the results of an initiative to transmit imagery content through a Link-16 tactical network using JPEG2000 compatible approach (involving wavelets to compress images). Specifically, the JPEG2000 code-stream is mapped into Link-16 free-text messages. The most important part of the JPEG2000 compressed image is transmitted through a more error resistant (and anti-jamming) Link-16 packed structure and the remaining of the image in less robust data structures but at higher data rates. The results presented are preliminary and dependent on Link-16 network resources.

The need for high compression and artifacts free imaging has made JPEG2000 a capable and sustaining algorithm that is replacing the current JPEG which is applied and used till today [7]. The discrete version of Wavelet Transform in two dimensions is called two dimensional discrete wavelet transform (2-D DWT). The implementation requires digital filters and down-samplers. In JPEG2000, typically images are decomposed to five wavelet levels to accomplish higher compression ratio. In multimedia communication and data storage, the drawback of compression is that the compressed data are vulnerable to channel noise during transmission. The area of compressed data transmission through noisy channels is still active in research, and needs further investigation. On the other hand, authentication of transmitted data is equally important to justify all image transmission related activities. Recently, protection of image data transmitted or stored over open channels is also getting serious attention.

The paper is structured as follows. In the next section, the literature review is presented to highlight important contributions to this area of research. The section III details proposed approach. In section IV, the experiments conducted on test images are discussed and results presented. The section V presents discussion on these test results, followed by conclusions in section VI.

2 LITERATURE REVIEW

Typically, watermark techniques protect the right of service providers, while digital signature covers customers. As an example, a customer wants to verify the seller of the image and that the purchased image is in fact bought from the legal one. In this case, digital signature comes as a useful tool. In terms of approaches, for example, in [8], the authors investigate the invariant features, which are generated from fractionalized bit-planes during EBCOT (Embedded Block Coding with Optimized Truncation) procedure in JPEG2000. These are then coded and signed by the sender's private key to generate one crypto signature (hundreds of bits only) per image, regardless of the image size. The authors in [9] discuss a scheme, where scalability and robustness is achieved by truncating bit planes of wavelet coefficients into two portions in JPEG2000 codec based on lowest compression bit rate (CBR). The invariant features, which are generated from upper portion, are signed by the sender's private key to generate a crypto-signature. By embedding the signature in upper portion, the scheme has the ability for content authentication as long as the final transmitted bit rate of the image is not less than the lowest CBR. In another work [10], a secure encryption scheme is proposed, where only some sensitive

precincts of the entire image are encrypted. Thus, the code stream is parsed to select only packets containing code-blocks which belong to the selected precincts. The remaining packets are sent without encryption.

The authors in [11] select LL coefficients as authentication code (AC) since root nodes preserve the most important energy. To embed AC in image with imperceptibility, AC is further scaled and rearranged into bit planes. The embedding procedure inserts the AC bit plane into multi-resolution images according to progressive image transmission. In [12], the authors employ Dugad technique [13] to resolve security issues in medical images by adding watermark technology to JPEG2000 compression. The authors in [14] have proposed watermarking and image authentication scheme to be performed in the frequency domain (with DCT coefficients). The authors claim to integrate ownership (through watermarking) and integrity of the image through signature process.

In [15], the main features of the proposed authentication system include integration of both content based (semi-fragile) authentication and code-stream based (complete) authentication into one unified system. This gives users more freedom to choose a proper type of authentication according to their specific requirements in the application.

Scrambling and Encryption: Recently, a great deal of concern has been raised regarding the security of an image transmitted or stored over public channels. The authors in [16] have proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. In another work [17], a neural network based encryption has been suggested as a part of encryption and decryption. At the receiving end, it uses neural network to obtain the original image. Scrambling has also been investigated by many authors for example in [18], where authors achieve encryption by dividing the image into random overlapping square blocks, generating random iterative numbers and random encryption order, and scrambling pixels of each block using Arnold transform. In another work [19], the authors use fast image scrambling algorithm using a multidimensional orthogonal transform and a cipher image. The security is achieved by a large number of multi-dimensional orthogonal sequence. The authors in [20] use wavelet decomposition to apply encryption on high-frequency sub-band image. After that, wavelet reconstruction is introduced in order to spread the encrypted part throughout the whole image. A second encryption process follows to complete the encryption process.

Noise Removal: Once data is received at the receiver, errors are detected and if possible, they are also corrected. Since compressed data are more vulnerable to channel noise, therefore, the transmitted data must be resilient to channel noise and other impairments. The techniques to address this problem have been classified into three groups. The first technique is Forward Error Concealment in which the encoder makes the data more immune to transmission errors with the objective to decrease corresponding effect to a minimum. The second technique is

error concealment by post processing, where the decoder a major job in concealing errors without depending on additional data from the encoder. The third technique is interactive error concealment (IEC) in which the encoder and decoder work jointly through a feedback channel to minimize the impact of transmission errors. As a reference, various error concealment errors are discussed in [21].

Summary of Issues: Though image authentications techniques have grown to be mature technologies, but the current state of the art approaches do not completely solve the problem of unauthorized copying, provide protection from digital data privacy and image authentication through noisy channel. Furthermore, there exist many image editing applications that enable easy manipulation of image data, and this problem becomes serious in applications like medical imaging and area surveillance. In this work, an approach is investigated that collectively addresses security and privacy of (compressed) image data transmitted through noisy channels. Noise removal and image authentication at different levels are the main contributions of this work.

3 PROPOSED APPROACH

In this section, an approach as shown in Figure 1 is presented that achieves two major objectives in image transmission: (i) embeds authentication in JPEG2000 image before transmission, (ii) uses edge image to help in identifying corrupted regions, in the receiver. Each of the steps, as shown in Figure 1, is discussed as follows:

3.1 Edge Extraction

Edge detection is the most useful approach in detecting valuable or important changes in the value of the intensity. This kind of detection is achieved using first order or second order derivative of intensity values. When there is a change in the intensity, the direction of the gradient vector can be determined by calculating the angle of the maximum rate of change. This also means that where ever there is a detection of an edge, there is going to be an important difference between the pixels. This kind of difference denotes the level variation between intensity densities. Moreover, one of the reasons that could make this variation high is the existence of high frequency (noise) at that area. At the transmitter, the N_L -scale wavelet transform is applied as a first step in JPEG2000 coding standard, and the edge image is extracted from these wavelet coefficients. For the purpose of edge detection, Canny edge detector [22] with convenient thresholds is applied to the wavelet transformed image. The resulting binary edge_image undergoes scrambling to protect data and lossless compression to minimize transmission overhead through noisy channel, as discussed below.

3.2 Scrambling

In literature [23], it has been shown that block level scrambling provides better results than pixel based scrambling, and that it is computationally efficient. For the same purpose, sub-bands of the edge image are decomposed into non-overlapping blocks of pixels, with block size

dependent on the level of scrambling. In the next step, these blocks are permuted using 2-D Arnold transform, and these permutations again depend on the level of scrambling. The 2-D Arnold transform is given as [23]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & 1+ab \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } (N) \quad (4)$$

where N is the order of the image matrix, and a, b being positive control parameters are further randomly generated through 2-D coupled logistic map, given below:

$$\begin{aligned} x_1(n+1) &= \mu_1 x_1(n) (1 - x_1(n)) + \gamma_1 x_2^2(n) \\ x_2(n+1) &= \mu_2 x_2(n) (1 - x_2(n)) + \gamma_2 (x_1^2(n) + x_1(n)x_2(n)) \end{aligned} \quad (5)$$

This logic map has three coupling terms to show its complexity. It is shown in [23] that the map is chaotic if $2.75 < \mu_1 \leq 3.4$, $2.7 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$, $0.13 < \gamma_2 \leq 0.15$. Thus, the chaotic sequence in equation (5) is generated for $0 < x_1, x_2 < 1$, and then a , and b are generated through x_1 and x_2 . Once a , and b are generated, then equation (4) is applied on blocks of each sub-band of the edge image, up to k -level scrambling, to get the overall scrambled image. Since the steps of this scrambling are deterministic, it seems easy to apply it in reverse order to descramble image at the receiver. It should be noted that since higher subbands of the edge image contain relatively little visual information about the edge, hence scrambling can only be applied to lower band subbands and leaving higher subbands untouched.

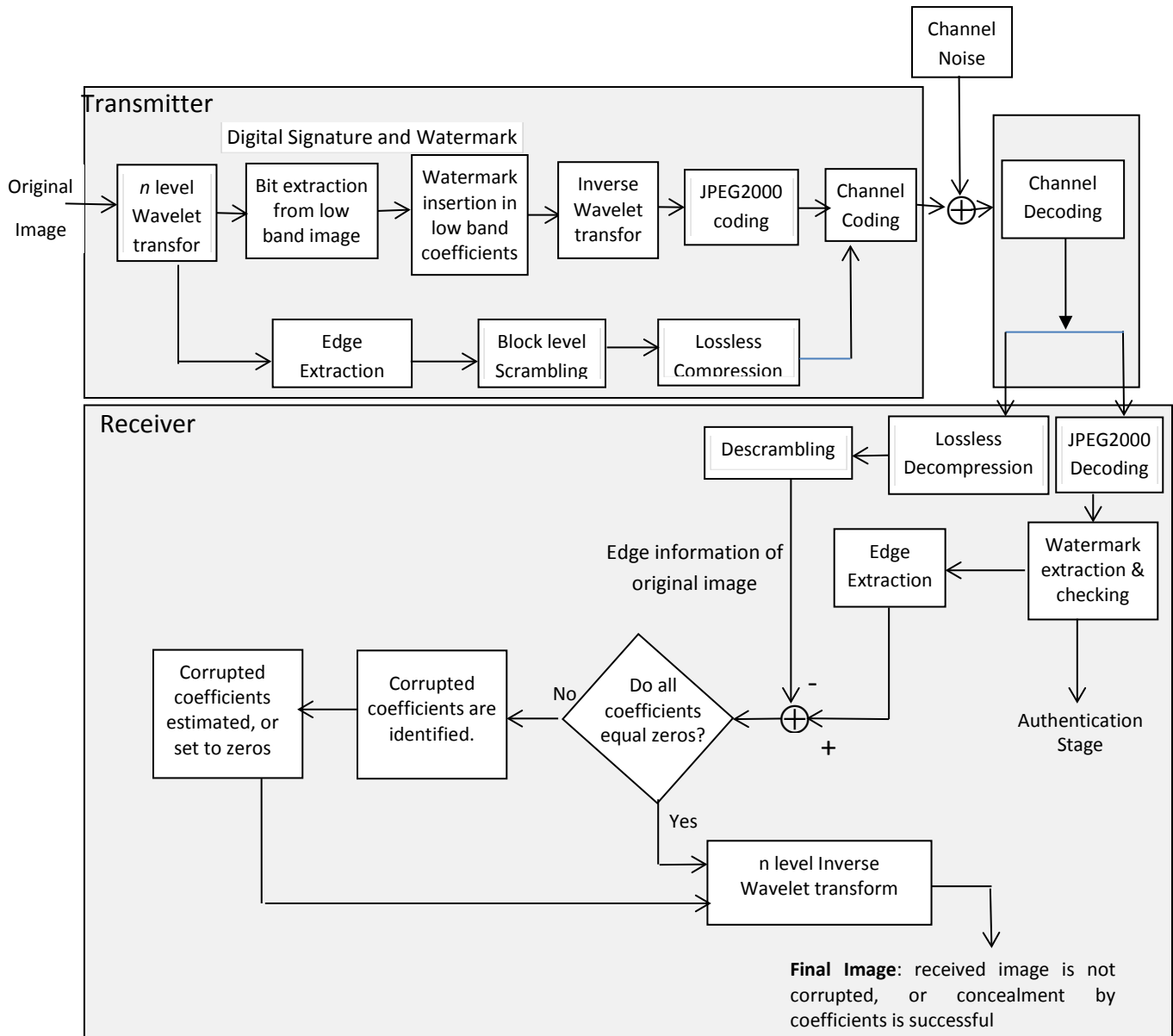


Figure 1: Block diagram of Proposed Algorithm

3.3 Lossless Compression:

The objective of this step is to reduce the size of overhead that results due to transmission of the encrypted edge_image. The lossy approach can't be used here as the edge image is to be used for error concealment in the received image, thus any lossless compression scheme that reduces the size of this overhead can be used. Since higher subbands of the edge image contain a lot of zeros, the lossless compression of these bands would yield a bigger compression gain. In this approach, run length encoding is adopted for simplicity. The idea is pick up identical patterns present in the binary edge image and represent them as nd , where n is the number of consecutive occurrences, and d is the data string.

3.4 Embedding Authentication:

In order to present digital signature extraction and watermark insertion into image, it seems reasonable to define parameters. For simplicity, we assume image and block of square size. Let original image $f(x, y)$ be of size $N \times N$, and its low band subband be represented as $LL_n(i, j)$, where n represents the decomposition scale of the image and i, j are indices of the image band in the range $0 \leq i \leq N/2^n$ and $0 \leq j \leq N/2^n$. In order to extract digital signature from the image, it is proposed to divide the lowest image subband into blocks S_k ($k=1, 2, 3, \dots, M$) to enable bit extraction across whole subband image. The total extracted number of bits is $M \times L$, where L is number of bits generated per block. Moreover, it seems satisfying for customers and image providers to have content dependent digital signature extracted from within the image rather than selecting external bits as digital signature, and sent separately across the channel. These extracted bits are later inserted as watermark in the same subband. Though the approach of digital signature extraction and its insertion as watermark may help in detecting channel manipulation of bits at the receiver, but at the moment it is not addressed in this approach.

3.5 Digital Signature

The digital signature extraction is based on two main points: (a) any low band image coefficient cannot be made larger or smaller without causing significant perceptual changes to the image, thus all similarly looking blocks (whether watermarked, un-watermarked, or attacked) in the wavelet transformed low band image will have same signature bits (b) a variable threshold is used in generating bits from the low band image blocks in such a way that 50% of the projections lie on either side of the threshold to ensure maximum information content in extracted bits. The adaption of the threshold is done to counter changes in information content from block to block due to data manipulations, for example certain image processing operations such as histogram stretching, watermarking, noise adding, compression, filtering, etc. In order to extract bits from low band subband, a secret key K (to be chosen, say by image provider or author) is used to generate L random sequences with values uniformly distributed in the interval $\{0, 1\}$. These matrices are later smoothed out by a low pass filter, and made zero mean to represent subband variations only. Later, image block S_k , as a vector, is projected on each zero mean smoothed random pattern L_i , and then its absolute value is compared with a threshold to generate corresponding bit c_i , as follows:

$$\begin{aligned} c_i &= 1, \text{ if } |S_k \cdot L_i| > 0 \\ c_i &= 0, \text{ if } |S_k \cdot L_i| < 0 \end{aligned} \tag{6}$$

Based on this approach, it can be easily seen that (i) resulting projected values change with a change in K (ii) resulting projected values change if S_i is dissimilar than S_j where $i \neq j$. Thus, bits c_i are sensitive to key K and vary continuously with subband block S_k .

3.6 Watermarking

As described above, the signature bits that are extracted from LL_n are inserted back as watermark in the lowest subband. This is ensured by using a quantization process, and mean amplitude of the lowest subband. Furthermore, it is desired that inserted watermark be extracted without having access to the original image, and that process be robust against common image processing application such as JPEG compression. Mathematically, watermarking process can be described as:

$$LL'_n = W_F(LL_n, c, K) \quad (7)$$

where LL'_n , W_F , LL_n , c , K represent watermarked subband, watermark (forward) coding process, unwatermarked subband, signature bits and key respectively. Similarly, the inverse process can be described as:

$$c' = W_R(LL'_n, K) \quad (8)$$

where c' and W_R represent recovered bits and watermark (reverse) coding process respectively. Finally, c and c' go through similarity index check using a threshold T_2 to determine whether correct watermark has been recovered.

For embedding watermarking bits into the subband, the procedure starts as follows:

- i. Select embedded intensity as a quantization step size B_t , and calculate the mean m_k of each block S_k . Set $b_k = \text{int} [m_k/B_t]$.
- ii. Compute the difference diff_k as:

$$\text{diff}_k = \text{abs} (b_k - \text{trunc} [m_k/B_t])$$
- iii. Modify b_k using c_k , b_k and diff_k as:
If b_k is an odd number and $c_k = 0$,
OR if b_k is an even number and $c_k = 1$, then

$$b'_k = \{ b_k + 1 \text{ for } \text{diff}_k = 0$$

$$b_k - 1 \text{ for } \text{diff}_k = 1 \} \text{ else } b'_k = b_k$$
- iv. Update wavelet coefficients of block S_k of $LL_n(i, j)$ as:

$$LL_{nk}(i, j) = LL_{nk}(i, j) + (b'_k \times B_t - m_k)$$

where $LL_{nk}(i, j)$ stands for wavelet coefficient (i, j) of block S_k in lowest subband.
- v. Compute and save new mean m_t of $LL'_n(i, j)$, and construct watermarked image using inverse wavelet transform.

Once the image arrives at the receiver, the watermarked bits are extracted as follows:

- i. The mean m_r of the received lowest subband $LL_n^-(i, j)$ is calculated, and difference is computed as:

$$\delta_m = m_r - m_t$$
- ii. The received lowest subband $LL_n^-(i, j)$ is decomposed into blocks S_k^- and mean m_k^- is calculated.
- iii. Compute the quantization value as:

$$B_r = \text{int} [(m_k^- - \delta_m) / B_t]$$

- iv. Extract the embedded bit as:
If B_r is even, then $c_k = 0$, else $c_k = 1$.

3.7 JPEG2000 and Channel Coding

Once the watermarked image is available, it is ready for JPEG2000 coding and transmission through noisy channel. Furthermore, scrambled and lossless compressed edge image is also ready for transmission through the same channel. As the size of compressed edge image is significantly lower than the original image, it can be coded using robust channel coding schemes to void distortion due to noise. Thus it is assumed that it is correctly received at the receiver. So at the receiver, watermarked-noisy-compressed image and noise free lossless-compressed edge image are received. The channel noise assumed is the burst noise i.e., the two-state Markov channel model is used to represent bursty noise channel. This noise is added to transmitted data before it reaches the receiver.

3.8 Receiver operations

The receiver steps follows exactly as shown in Figure 1. The steps just invert the operations stated in sections *e*, *d*, *c*, *b*, and *a* respectively. Once edge is extracted from wavelet coefficients image, it is termed as extracted edge image respectively. Next extracted edge image is subtracted from the received edge image of the original image. If the difference between the received edge image and the extracted edge image is zero or below a certain threshold level then the received image is correct or corruption is unobjectionable. In the case where the received edge image differs from the extracted edge image at different regions, these regions are marked as corrupted regions. In JPEG2000, the corrupted regions will have different sizes since the wavelet coefficients at different levels represent different sizes of blocks in the reconstructed image. The block sizes can range from 2 by 2 pixels to 32 by 32 pixels, and generally this depends how many levels of wavelet transform are computed at the transmitter. The spatial pattern of the corrupted region may help to determine if the corrupted region is in the horizontal, vertical, or diagonal *sub-band*.

Concealing errors at higher *sub-band*: This step deals with existence of the corrupted regions or blocks in received wavelets coefficients. The location of the corrupted block in the received wavelet coefficients may be used to determine the location of the wavelet coefficient within the *sub-band*. Effectively, all of these sub-bands may be processed in parallel to determine corrupted wavelet coefficients. Once it is possible to locate the corrupted wavelet coefficients, then their values may be set to zero if the coefficients belong to higher sub-bands at higher level lower level or may be estimated by adjacent coefficients if the coefficients belong to higher sub-bands at lower level. Then the image is reconstructed. The loss of image information by setting the values of the wavelet coefficients to zero is unobjectionable especially for coefficients located at higher *sub-bands*.

Concealing errors at lower *sub-band*: If the corrupted coefficients are in the lower *sub-band* then it is proposed to estimate their values from the neighborhood of affected coefficients. For example, if the corrupted coefficients are the approximation coefficients, then it is proposed to estimate their values using the uncorrupted adjacent approximation coefficients.

4 EXPERIMENTAL SETUP AND RESULTS

A set of five 1024×1024 8-bit monochrome images were selected based on various image details to test the approach presented in the previous section. The Figure 2 shows these images: *woman* and *pirate* images (with low image detail), *boat* and *goldhill* (with medium level of detail) and *baboon* image (with large image detail). All of these images were transformed using an arbitrary five-scale ($N_L=5$) wavelet transform with implicit quantization $\mu_0=8$ and $\varepsilon_0=8.5$.

A canny edge detector with convenient thresholds was applied on wavelet coefficients sub-images in order to extract the edge image. The resulting binary image, termed as 'edge_image' undergoes scrambling. It should be noted that, as discussed in previous section, only lowest subband undergoes scrambling. Once initial block size is selected, at each level the blocks are permuted using the equation 4. The arbitrary values (to be used in equation 5) for initial conditions and parameters for secret key selected were: $x_0=0.0215$, $y_0=0.5734$, $\mu_1=2.93$, $\mu_2=3.17$, $\gamma_1=0.197$, $\gamma_2=0.139$, and $t=100$. The values a and b are then generated as in [23]. The final scrambled image is reached once number of levels starting from $y=1$ reaches $\log_2(Y)-1$, where Y is the initial block size.. All variables were set to double with 15-digit precision, and decimal fractions of the variables are multiplied by 10^{14} . The scrambled subbands levels together with remaining binary edge image subbands were then losslessly compressed using run length coding.

The next step on the transmission side is to embed authentication in the image. As discussed in the previous section, only lowest subband is to be used for digital signature extraction and watermark insertion. For signature extraction, first the lowest subband image is divided into blocks of arbitrary size of 8x8 pixels, thus generating 16 blocks. Using an author name as secret key, $L=32$ random sequences were generated with values uniformly distributed in the interval $\{0, 1\}$, followed by smoothing, and zero mean steps. Each subband block is finally projected onto each random sequence (and using equation 6) to generate a total of $16 \times 32 = 512$ signature bits. In order to insert these signature bits back into lowest subband as a watermark, the quantization step size was arbitrarily selected as $B_t = 10$. Using the watermarking algorithm stated in previous section, the wavelet coefficients of each block in the lowest subband are modified. The mean m_t of resulting coefficients in the lowest band is also saved. Finally, inverse wavelet transform is applied on the modified wavelet coefficients together with remaining subbands to generate watermarked image.

The watermarked image finally undergoes JPEG2000 coding using an arbitrary five-scale ($N_L=5$) wavelet transform, with implicit quantization $\mu_0=8$ and $\varepsilon_0=8.5$. The resulting JPEG2000 coded

image together with mean value m_t and edge image were channel coded before transmission. The size of wavelet coefficients resulting from JPEG2000 coding and watermarked image together with mean value is 1024KB, whereas edge image size is \sim 3KB only. Since edge image is required to be with zero distortion at the receiver, this is coded with channel coding technique to withstand noise in the channel. This step added up to 5KB extra to the edge image. The added noise to the channel is the burst noise, which was simulated by two-state Markov channel model. After generating the two-state Markov noise, this noise (with bit error rate equal to 0.004, 0.006, 0.009 to represent different noise scenario) was added logically to the binary Huffman coded data. The method of addition was done simply by applying the exclusive OR logical operation and the result was an image with noise distortion. The image mixed with noise is transmitted using JPEG2000 protocols and was the one received at the receiver.



Figure 2: Test images (a) woman (b) pirate (c) goldhill (d) boat and (e) baboon

After data is channel decoded, two images are available. One is the lossless compressed image that undergoes inverse operations done at the transmitter. Firstly, it undergoes lossless decompression followed by descrambling exactly in reverse order of transmission. Since this image was channel coded using a robust channel code, hence there was no distortion in the received edge image. On the other end, the second image was JPEG2000 decoded, followed by watermark extraction. Using the algorithm stated in previous section, the watermark bits were extracted. The method used to validate authentication of received image included number of mismatched bits exceeding a predefined threshold T_2 . It was found out that in all cases of noise (for all images), the bits were recovered with an average of 96.8% accuracy. It must be noted here that distortion in the received image included noise in the channel, imprecision added due to watermark, and JPEG2000 coding/compression. With various levels of compression, it was noted that as compression rate increased, watermark bit extraction success rate decreased.

However, higher scale decomposition used in wavelet transform improved the success rate as bits diffused from lowest scale to full image size. The quantization step size also affected the quality of the watermarked image i.e., the higher the quantization level, higher the degradation observed in all of the test images.

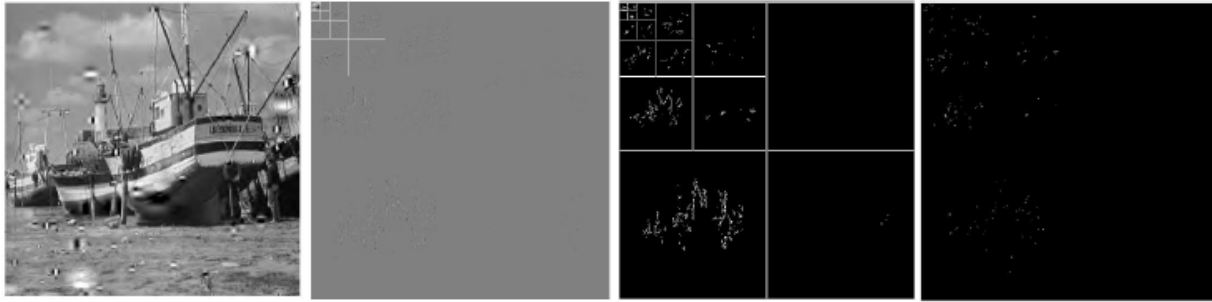


Figure 3: (a) Top left: Original image received with BER=0.009 (b) Top right: The displayed wavelet coefficients (c) Bottom left: Edge extraction of received wavelet coefficients (d) Bottom right: Result of subtracting extracted_edge_image from the received edge_image

Once watermark authentication is completed, edge image from received wavelet coefficients is computed. This image is termed as ‘extracted_edge_image’. This new extracted_edge_image is then subtracted from the received ‘edge_image’ to determine the corrupted regions resulting due to distortion in transmission channel. As an example, the Figure 3(a) shows the received image reconstructed after passing through noisy transmission channel with $BER = 0.009$. The Figure 3(b) shows the displayed wavelet coefficients of the received image, the Figure 3(c) shows the edge extraction of displayed wavelet coefficients, and the Figure 3(d) shows the location of the corrupted regions resulting by subtracting the extracted_edge_image of received coefficients from the received edge_image of coefficients of the original image.

In order to minimize distortion in the reconstructed image, error concealment method was adopted to handle corrupted regions in wavelet coefficients domain. In this work, selective corrupted regions are processed for error concealment, though the approach can be extended to all subbands. As an implementation, all corrupted coefficients for all sub-bands on level 5 are estimated using a median filter [24] on 3x3 neighborhood of the corrupted coefficient. The filter selection and its neighborhood size was arbitrary. The rest of corrupted coefficients on the higher sub-bands were simply set to zero. Once corrupted region coefficients are identified and estimated, the inverse wavelet transform is applied to reconstruct image. This approach was repeated on all five test images with different bit error rates, and the result for one image is shown in Figure 4. It seems clear that the proposed approach does conceal errors introduced in the noisy channel. In order to judge quality of reconstructed images, root mean square error (*rms*) and peak signal-to-noise ratio (PSNR) were calculated for test images against different BER values. Mathematically, this is described as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{mse} \right) \quad (9)$$

where *mse* stands for mean square of the difference between the original and reconstructed image. From results shown in Table 1, it is clear that almost all distortion due to channel noise have been removed due to error concealment and quality images restored. It can easily be inferred from Table 1 that as BER increases, *rms* values get increased. However, after concealment, these values are largely reduced. Likewise, PSNR values improved after concealment, with improvement ranging from 10-15 decibels.

Table 1: The *rms* and *PSNR* values for test images with channel BER=0.004, 0.006, 0.009

<i>Woman image</i>	Received Image		Concealed Image	
	<i>RMS</i>	<i>PSNR (dB)</i>	<i>RMS</i>	<i>PSNR (dB)</i>
BER=0.004	5.24	33.51	1.15	46.62
BER=0.006	6.39	32.18	0.98	48.18
BER=0.009	9.85	28.25	2.85	38.76
<i>Pirate image</i>	Received Image		Concealed Image	
	<i>RMS</i>	<i>PSNR (dB)</i>	<i>RMS</i>	<i>PSNR (dB)</i>
BER=0.004	11.68	26.95	1.67	43.48
BER=0.006	13.56	25.52	3.41	36.25
BER=0.009	14.21	25.69	2.15	41.11
<i>Boat image</i>	Received Image		Concealed Image	
	<i>RMS</i>	<i>PSNR (dB)</i>	<i>RMS</i>	<i>PSNR (dB)</i>
BER=0.004	8.58	29.52	2.11	41.69
BER=0.006	11.72	26.40	3.54	37.11
BER=0.009	17.32	23.41	2.67	39.57
<i>Goldhill image</i>	Received Image		Concealed Image	
	<i>RMS</i>	<i>PSNR (dB)</i>	<i>RMS</i>	<i>PSNR (dB)</i>
BER=0.004	9.25	28.75	3.96	36.02
BER=0.006	9.38	28.59	1.87	42.18
BER=0.009	10.71	27.64	2.38	40.44
<i>Baboon image</i>	Received Image		Concealed Image	
	<i>RMS</i>	<i>PSNR (dB)</i>	<i>RMS</i>	<i>PSNR (dB)</i>
BER=0.004	7.48	30.73	2.37	40.45
BER=0.006	8.57	29.49	3.21	38.51
BER=0.009	10.61	27.57	3.50	37.09

5 DISCUSSIONS

The objective of this research was to supplement transmission of JPEG2000 image data with authentication and noise handling capability. Image authentication method proposed in this approach was to counter unauthorized manipulations in the image. The lowest subband was used to extract signature bits and place watermark inside. The purpose behind content driven signature extraction was simplicity as opposed to different signature taken from the author or the publisher. It was found out that as number of decomposition levels increases, so is the diffusion rate of this watermark within the whole image after reconstruction. The authentication level at the receiver can be adjusted based on how much percentage of error is allowed.

The edge image was used to tackle channel distortion. In order to ensure minimum overhead on transmission, and noise free reception at the receiver, it was scrambled, lossless compressed and then followed by channel coding. Though it causes overhead, but it provides tradeoff with respect to visual quality of the image. Besides, this overhead is minimal as total overhead amounts to few kilo bytes. This step is optional and can be removed if channel has least noise distortion.

The advantages gained through proposed approach can be compared, for example, with the approaches described in [8-11]. In [8], the authors discuss digital signature extraction scheme for semi-fragile content through combination of hashing, public/private key for digital signature, and transmission of watermarked image along with cryptographic signature. The approach proposed in our paper is generic and more flexible than the one in [8], because it is independent of public/private infrastructure, and carries noise concealment ability. Similarly, the approach in [10] targets only medical images and encrypts some of the JPEG2000 coded image data using permutations, and remaining image data is not processed. This approach only fits some local network applications that secure only partial content. Likewise, the approach in [9] embeds watermark in the JPEG coded image using private key and lowest compression bit rate. There is no immunity against noise or how the encrypted image is degraded by noise. Additionally, there is no way to know regions where degradation or tampering may have occurred. In [11], the authors propose watermarking scheme for progressive image transmission along with compensation mechanism to reduce embedding distortion. This approach considers low band coefficients, and uses it as an authentication code to be embedded into other bands. It fails to consider effects of noise during transmission and how this noise affects compensation algorithms proposed in [11]. The approach is not generic and fits only an specific application.

6 CONCLUSIONS

An image authentication approach was proposed in this research that embedded content driven digital signature as a watermark before JPEG2000 coding. A separate edge

image data was integrated with image authentication as a supplement to offset effects of noisy channel on image transmission. Effectively, edge image data added turned out to be very small of about 0.78% fraction of the actual image data. The approach provides system robustness, security, and better visual quality. Three advantages were clearly noted: (a) the selected data for scrambling and that for signature extraction and watermarking was small resulting in reduced computational complexity (b) data rate remains unchanged as effectively individual coefficients in selected subbands were replaced by equivalently by same number of new modified values (c) noise concealed by this approach is significant compared to overhead cost of about 0.78% on transmission.



Figure 4.: The received and concealed images for boat image: Top: (a) and (b) for BER=0.004; Middle: (c) and (d) for BER=0.006; Bottom: (e) and (f) for BER=0.009

ACKNOWLEDGMENTS

The author would like to express sincere thanks to the Research Affairs unit of College of Engineering at United Arab Emirates University for financial support of this project under grant code number EE-21N151.

REFERENCES

- [1]. S. Khalid, Introduction to Data Compression, New York, Morgan Kaufmann Publishers, 2000
- [2]. L. Hanzo, P. Cherriman, J. Streit, Wireless Video Communications: *IEEE Series*, NY: IEEE Press, 2001.
- [3]. Y. Wang and Q. Zhu, "Error control and concealment for video communication: A Review," *Proceedings of the IEEE*, Vol. 86, No. 5, pp. 974-996, May 1998.
- [4]. Qurban Memon, "A New Approach to Video Security over Networks", *International Journal of Computer Applications in Technology*, Vol. 25, No. 1, 2006, pp. 72-83.
- [5]. Mairal, C. and Agueh, M. , "Scalable and robust JPEG 2000 images and video transmission system for multiple wireless receivers", *2010 IEEE Latin-American Conference on Communications (LATINCOM)*, ECE, LACSC, Paris, France.
- [6]. Martinez-Ruiz, M., Artes-Rodriguez, A., Diaz-Rico, J.A., Fuentes, J.B., "New initiatives for imagery transmission over a tactical data link. A case study: JPEG2000 compressed images transmitted in a Link-16 network method and results", *Military Communications Conference*, 2010, pp. 1163-1168.
- [7]. P. Schelkens, A. Skodras & T. Ebrahimi. The JPEG 2000 Suite. Wiley, Series: Wiley-IS&T Series in Imaging Science and Technology, 2009.
- [8]. Sun, Q., "A Secure and Robust Digital Signature Scheme for JPEG2000 Image Authentication", *IEEE Transactions on Multimedia*, Vol.7, No.3, pp.480,494, June 2005, doi: 10.1109/TMM.2005.846776
- [9]. Wen, J., Wang, J., Feng, F., Zhang, B., "A Reversible Authentication Scheme for JPEG2000 Images", *The Ninth International Conference on Electronic Measurement & Instruments*, vol., no., pp.4-486,4-489, 16-19 Aug. 2009
- [10]. Zahia Brahimi, Z., Bessalah, H., Tarabet, A., Kholadi, M., "A new selective encryption technique of JPEG2000 codestream for medical images transmission", *5th International Multi-Conference on Systems, Signals and Devices*, 2008.
- [11]. Tsai, P., , Hu, Y., Yeh, H., Shih, W., "Watermarking for Multi-resolution Image Authentication", *International Journal of Security and Its Applications* Vol. 6, No. 2, April, 2012.
- [12]. Lim,,S., Moon, H., Chae, S.,, Yongwha Chung, Y., Pan, S., "JPEG2000 and Digital Watermarking Technique Use in Medical Image", *IEEE International Conference on Secure Software Integration and Reliability Improvement*, pp. 413-416, 2009

- [13]. R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-based Scheme for Watermarking Images", *Proceedings of IEEE International Conference on Image Processing*, Chicago, IL, USA, Oct. 1998, 419-423.
- [14]. Kung, C., Chao, S., Yan, Y., Kung, C., "A Robust Watermarking and Image Authentication Scheme used for Digital Content Application", *Journal of Multimedia*, Vol. 4, No. 3, June 2009, pp. 112-119
- [15]. Sun, Q., Zhang, Z., "A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking", *China Communications*, pp. 71-80, October 2006
- [16]. Sathishkumar , G., Ramachandran, S., Bagan, K., "Image Encryption Using Random Pixel Permutation by Chaotic Mapping", *IEEE Symposium on Computers and Informatics*, 2012, pp. 247-251
- [17]. Joshi, S., Udupi, V., Joshi, D., "A Novel Neural Network Approach for Digital Image Data Encryption/Decryption", *IEEE International Conference on Power, Signals, Controls and Computation*, pp.1-4, 3-6 January, 2012
- [18]. Tang, Z., and Zhang, X., "Secure Image Encryption without Size Limitation using Arnold Transform and Random Strategies", *Journal of Multimedia*, Vol. 6, No. 2, April 2011, pp. 202-206
- [19]. Li, S., Wang, J., Gao, X., "The Fast realization of Image Scrambling Algorithm using Multi-Dimensional Orthogonal Transform", *IEEE Congress on Image and Signal Processing*, pp. 47-51, 2008
- [20]. Yu, Z., Zhe, Z., Haibing, Y., Wenjie, P., Yunpeng, Z., "A Chaos-Based Image Encryption Algorithm Using Wavelet Transform", *2nd International Conference on Advanced Computer Control*, Vol.2, pp. 217-222, 27-29 March, 2010
- [21]. Y. Wang and Q. Zhu, "Error control and concealment for video communication: A Review," *Proceedings of the IEEE*, Vol. 86, No. 5, pp. 974-996, May 1998
- [22]. J. Canny, "A Computational Approach to Edge Detection," *IEEE Transactions on Pattern Analysis*, Vol. PAMI-8, No. 6, pp. 679-698, Nov. 1986.
- [23]. Musheer Ahmad, A., Haque, E., Farooq, O., "A Noise Resilient Scrambling Scheme for Noisy Transmission Channel", *International Conference on Multimedia, Signal Processing and Communication Technologies*, pp. 91-94, 2011
- [24]. Memon, Q., Kasparis, T., "Block median filters", *International Symposium on OE/Aerospace Sensing and Dual Use Photonics*, pp. 100-109, Orlando, 1995.